UNIVERSIDAD AUTÓNOMA DE MADRID
ESCUELA POLITÉCNICA SUPERIOR
DEPARTAMENTO DE TECNOLOGÍA ELECTRÓNICA Y DE LAS COMUNICACIONES

IMPROVING SECURITY AND PRIVACY IN BIOMETRIC SYSTEMS

–TESIS DOCTORAL–

MEJORA DE LA SEGURIDAD Y LA PRIVACIDAD DE LOS SISTEMAS BIOMÉTRICOS

Author: Marta Gómez Barrero

(Ingeniero de Informática y Licenciada en Matemáticas, Universidad Autónoma de Madrid)

A Thesis submitted for the degree of:

Doctor of Philosophy

Madrid, April 2016

Colophon

This book was typeset by the author using LaTeX2e. The main body of the text was set using a 11-points Computer Modern Roman font. All graphics and images were included formatted as Encapsuled Postscript (^{TM} Adobe Systems Incorporated). The final postscript output was converted to Portable Document Format (PDF) and printed.

This Thesis was printed with the financial support from EPS-UAM and the Biometric Recognition Group-ATVS.

Department:	Tecnología Electrónica y de las Comunicaciones Escuela Politécnica Superior Universidad Autónoma de Madrid (UAM), SPAIN
PhD Thesis:	Improving security and privacy in biometric systems
Author:	**Marta Gómez Barrero** Ingeniero de Informática y Licenciada en Matemáticas Universidad Autónoma de Madrid, SPAIN
Advisor:	**Javier Galbally Herrero** Doctor Ingeniero de Telecomunicación Universidad Autónoma de Madrid, SPAIN
Year:	2016
Committee:	President: **Javier Ortega García** Universidad Autónoma de Madrid, SPAIN
	Secretary: **Pablo Varona Martínez** Universidad Autónoma de Madrid, SPAIN
	Vocal 1: **Christoph Busch** Hochschule Darmstadt, GERMANY
	Vocal 2: **Julien Bringer** Morpho, FRANCE
	Vocal 3: **Fernando Pérez González** Universidad de Vigo, SPAIN

The research described in this Thesis was carried out within the Biometric Recognition Group – ATVS at the Dept. of Tecnología Electrónica y de las Comunicaciones, Escuela Politécnica Superior, Universidad Autónoma de Madrid (from 2012 to 2016). The project was partially funded by a PhD scholarship from Spanish Ministerio de Educación, Cultura y Deporte.

The author was awarded with a PhD scholarship "Formación de Personal Universitario (FPU)" from Spanish Ministerio de Educación, Cultura y Deporte between 2013 and 2016 which supported the research summarized in this Dissertation.

The author has been awarded with the Best Voted Poster Paper Award in the IAPR International Conference on Biometrics 2013: Marta Gomez-Barrero, Javier Galbally, Réjean Plamondon, Julian Fierrez and Javier Ortega-Garcia, "Variations of Handwritten Signatures with Time: A Sigma-Lognormal Analysis", Proc. of IEEE/IAPR ICB 2013, pp. 1-6, Madrid, Spain, June 2013.

The author was awarded with the "Archimedes" Award: Introduction to Scientific Research from Spanish Ministerio de Educación, Cultura y Deporte in 2013, for part of the research work originated from this Dissertation: Marta Gomez-Barrero, "Stealing Identities: New Attack to a Multimodal Biometric System".

The author has been awarded with the Siew-Sngiem Best Paper Award in the IAPR International Conference on Biometrics 2015: Marta Gomez-Barrero, Javier Galbally, Julian Fierrez, Javier Ortega-Garcia and Réjean Plamondon, "Enhanced On-Line Signature Verification Based on Skilled Forgery Detection Using Sigma-LogNormal Features", Proc. of IEEE/IAPR ICB 2015, pp. 501-506, Phuket, Thailand, May 2015.

The author was awarded with the EAB European Biometric Industry Award 2015, from the European Association for Biometrics, for part of the research work originated from this Dissertation: Marta Gomez-Barrero, "Fully Unlinkable and Irreversible Template Protection Based on Bloom Filters".

Abstract

The achievement of perfect security is out of the question. Even if we are not yet aware of them, every security aimed technology has weaknesses which attackers can exploit in order to circumvent the system. We should hence direct our efforts to the development of applications whose security level make it infeasible for computationally bound attackers to break the systems.

This Thesis is focused on improving the security and privacy provided by biometric systems. With the increased need for reliable and automatic identity verification, biometrics have emerged in the last decades as a pushing alternative to traditional authentication methods. Certainly, biometrics are very attractive and useful for the general public: forget about PINs and passwords, you are your own key. However, the wide deployment of biometric recognition systems at both large-scale applications (e.g., border management at European level or national identity systems) and everyday tasks (e.g., smartphone or PC access), has raised some concerns regarding the use and storage of such sensitive data. Therefore, understanding the threats which can affect those systems and analysing to what extent the subject's privacy is protected is of the utmost importance.

In this context, the present PhD Thesis pretends to shed some light into the difficult problem of security and privacy evaluation of biometric systems. To that end, a systematic analysis of the privacy provided by unprotected templates is carried out, and new biometric template protection schemes are proposed to deal with the unveiled privacy issues, being their robustness to the mentioned privacy threats thoroughly assessed. This way, the experimental studies presented in this Dissertation can help to further develop the ongoing standardization efforts on the assessment of template protection schemes.

The Thesis has been developed following the *security through transparency principle*, which has been largely applied in other security related areas such as cryptography. This paradigm relies on the fact that vulnerabilities exist regardless of their publication, and therefore pleads for making security systems as public as possible instead of keeping algorithms secret. This does not mean that obscurity cannot provide any protection. However, such a protection is in most cases only temporary. We should do our best to find threats and propose solutions to mitigate their effects. We believe that in order to grant the privacy protection that subjects are entitled to, it is necessary to understand and assess the threats, and publicly report quantitative analyses of their impact on the subject's privacy so that effective countermeasures can be developed.

Such privacy issues have already been acknowledged within the biometric community and numerous biometric template protection schemes have been proposed to tackle them. However, in most cases, thorough evaluations of the security and privacy provided by those systems are not carried out. In this Dissertation, after summarizing the most relevant works related to the Thesis, we describe the privacy and security evaluation methodology that has been followed

throughout the experimental chapters. These are dedicated to: *i*) the evaluation of unprotected templates and *ii*) the proposal and evaluation of biometric and multi-biometric template protection schemes, focusing on face, iris, fingerprint, handshape, fingervein and on-line signature, using publicly available biometric data and benchmarks in order to contribute reproducible research.

The experimental part of the Thesis starts with the security and privacy evaluation of unprotected biometric systems. To that end, the irreversibility of the templates is analysed posing ourselves the following question: starting from the information stored in the template, are we able to reconstruct synthetic samples which are positively matched to the stored references? To answer that question, we develop and implement two inverse biometric methods and use the reconstructed samples to launch attacks. Experiments show that it is indeed possible to fool handshape and iris based systems with those reconstructed images.

To address the privacy concerns raised by the previous study, we then propose a general framework for biometric and multi-biometric template protection based on Bloom filters. The proposed scheme not only prevents the reconstruction of synthetic biometric samples, but also deals with a second set of questions on privacy protection: can someone track my activities across different biometric verification systems? What if, for instance, my face based template is compromised: will I not be able to enrol in a system with my face ever again? A thorough experimental evaluation of face, iris, fingerprint and fingervein verification systems shows that the proposed scheme is able to protect the privacy of the subjects, even in the case secret keys are compromised and available to the eventual attacker. Furthermore, the scheme is robust to attacks based on known weaknesses of the underlying algorithms, preserving at the same time verification accuracy and speed.

Finally, as an alternative to the aforementioned scheme, we present a general framework for biometric and multi-biometric template protection based on Homomorphic Encryption. The security and privacy of the scheme is evaluated in an analogous manner for fingerprint and on-line signature verification, proving that the encrypted templates and all the operations carried out in the encrypted domain reveal no information about the underlying biometric data. Moreover, verification accuracy in the encrypted domain is equivalent to that achieved in the unprotected domain, and a similar verification speed can be achieved using fixed-length templates.

The research work described in this Dissertation has led to novel contributions which include the development of: *i*) a general framework for the security and privacy evaluation of biometric systems, and, in particular, for the unlinkability analysis of biometric templates, *ii*) two new methods to reverse engineer unprotected biometric templates, *iii*) a new biometric and multi-biometric template protection scheme based on Bloom filters, and *iv*) a new biometric and multi-biometric template protection scheme based on Homomorphic Encryption. Moreover, different original experimental studies have been carried out during the development of the Thesis. Besides, the research work completed throughout the Thesis has been complemented with the generation of several novel literature reviews and the improvement of current signature verification systems.

A mi familia.

Weisheit ist nicht das Ergebnis der Schulbildung,
sondern des lebenslangen Versuchs, sie zu erwerben.
(Wisdom is not a product of schooling,
but of the lifelong attempt to acquire it)
(La sabiduría no es un producto de la educación,
sino del intento de toda una vida por adquirirla)

Albert Einstein (1879–1955).

Acknowledgements

This PhD Thesis summarizes the work carried out during my Ph.D. studies with the Biometric Recognition Group - ATVS since 2012. This research group was established in 1994 at the Dept. of Ingeniería Audiovisual y Comunicaciones (DIAC) of the Universidad Politécnica de Madrid (UPM) and since 2004 is affiliated to the Dept. of Tecnología Electrónica y de las Comunicaciones of the Universidad Autónoma de Madrid (UAM). This Thesis has been mainly supported by a Ph.D. scholarship from Spanish MECD, which covered the period between March 2013 and April 2016, and also by various Spanish and European projects.

Foremost, I would like to give an special mention to my advisor Dr. Javier Galbally, who has continuously motivated me with his wise and intelligent advice, from the moment I started working at ATVS as an undergraduate student. It has been two and half years together in Madrid, and three years going long-distance, Madrid to Italy. I will never forget those multilingual emails full of knowledge, encouragement, and sound advice. And those Skype talks, always longer (and funnier) than expected. THANKS.

I would also like to thank Prof. Javier Ortega-García, Prof. Joaquin González and Dr. Julián Fiérrez, who opened the doors to their group for a challenging project when I was pursuing my Master's degree and who gave me the opportunity to get in touch with the research world. I really appreciate the confidence they have always shown in me. During these years I have benefited from their courage, self-mastery, and intelligent effort.

During the journey of my Ph.D. degree I have been fortunate to meet many excellent professionals and colleagues. I am especially grateful to Dr. Daniel Ramos and Dr. Pedro Tomé, two fellow researchers at ATVS who have continuously supported me, for their priceless advice and shared knowledge not only on academic topics.

But before them, a number of professors marked me during my years as an undergraduate student, specially Profs. Fernando Soria, Andrei Jaikin, Margarita Otero or José Dorronsoro. Your valuable lectures helped me keep on pursuing my degree no matter what, and awakened my interest in research in general, and machine learning in particular. And from my earlier school years, I cannot miss to mention Mario López González and Ezequiel Castellanos Maciá from IES Diego Velázquez, because of the many valuable things they taught me, which I will never forget. I would also like to thank José María Letona, for opening my eyes and mind to the wonderful world of mathematics and challenge solving.

Then, some of the best (academic and non-academic) moments of these last years took place far away from home, during my research stays. I would specially like to thank Prof. Christoph Busch for hosting me during my first internship, at the Biometric and Internet-Security Research Group (da/sec) in Darmstadt, Germany, and subsequently inviting me to the Norwegian Biometrics Lab in Gjøvik. Your guidance and support have been a key to the successful development of my Ph.D. Special thanks as well to Dr. Christian Rathgeb, with whom I have had the fortunate chance to collaborate for over three years and learn a lot in the meantime. *In dieser Zeit konnte ich nicht nur neue akademische Fähigkeiten erwerben, sondern auch mein Deutsch verbessern - Danke für eure Geduld!*

I would also like to thank Prof. Patrizio Campisi for hosting me at the Digital Signal Processing Multimedia and Optical Communications Laboratory at Università Roma Tre, in Italy, and making me feel at home, in spite of the hot Roman summer weather (very much eased in Ostia). I am grateful as well to Dr. Emanuele Maiorana and Dr. Marco Carli. Thanks for those morning chats, those coffee (*espresso*) breaks, for bearing my home-made meals (*lo so, solo manca il cioccolato a questa pasta, e mi dispiace! Forse dovrei ritornare a Roma e questa volta imparare come si mangia la pasta?*).

During those research stays, I had the chance to meet a huge number of colleagues, who soon became also friends. Apologizing to those I'm failing to mention here, I especially thank: Anika (my lab-mate for a month), Jessica (all happiness and joy), Martin Olsen (thanks for all those morning capuccinos that made my days), Xuebing Zhou (your nice gift reminds me of you anytime I see it!) and Christian (capuccinos are way better if accompanied by something sweet) from Darmstadt.

Those months in the cold Norway would have never been the same without the fantastic environment at HiG (thanks Patrick, Bian, Raghu, Slobodan, Hilde, etc.) or those great ski-weekends with Raymond, Luuk and Marian (exquisite Dutch chocolates!), Kiran (the fearless skier, and great beer buddy), Guoqiang (our personal waiter), Morten (PhD of life), Martin and Jasmina (*takk-og-takk!* as well for those wonderful dinners and for the Italian week) and Edlira (the other Mediterranean girl). And of course, big thanks to Christoph, the organizer and *langrenn* instructor.

From Rome, I hope to meet again (and soon) Gabriel (*grazie tante per tutti i consigli su Ostia... ma non dimenticare di non fissare i cani negli occhi!*), Emanuela (*peccato non avere il tempo per andare a Salisburgo!*) and Rig (sorry for those Spa-Italian confusing moments! *Cosa? A-si-...? ah! sí sí! Assisi! Bellissima!*).

And of course, I cannot forget to thank my two landlords, Rainer Witt and Giuseppe Parisi, and my not-so-Norwegian neighbour, Florissa Abreu - if it wasn't for your nice apartments and your immediate help any time I needed it, nothing would have ever been the same.

Big thanks to all of you, for achieving to make a madrileña feel at home in those long cold winter days, or in far too humid summer days.

Last but not least, I want to thank all the work mates at ATVS for all the good moments in the last six years, inside and outside the lab. So big thanks (in no particular order) to the older generation: Javier Franco (and his catchy jokes), Javier González (the Cervantes of the group), Pedro Tomé (no more *pelotitas*, please!), Rubén Vera (*el sevillano*), Ignacio López (our google-guy) and Daniel Ramos (awesome voice); the newest acquisitions: Rubén Tolosana (the n-th Rubén), Alicia Lozano (Dani Martín in love), Rubén Zazo (now that I thought no more *pelotitas* where coming at me...), Ester González-Sosa (our original *canaria*), Aythami Morales (our second *canario*); and to our international mates: Ruifang (*malita sijuan...*), Ram (our Indian guy), Rudolf (sorry, no more Hello Kitty here!) and Andreas (even if you don't like Spanish beer). And once again, thanks Galbally (*el cántabro*), for those wise talks (accompanied by videos) on some kind of extreme or snow-related sport, and those great jokes during lunch.

Y como siempre, lo mejor queda para el final: gracias a mi familia. Por estar ahí en lo bueno y en lo malo. Por no cesar de animarme en los momentos más duros, y de celebrar cada éxito, por pequeño que fuera. Sin mis padres, nada habría sido posible. Esto va por vosotros.

Gracias.

Marta Gómez Barrero
Madrid, March 2016

Contents

List of Figures

List of Tables

Chapter 1

Introduction

What happens if someone hacks a biometric database? Will the attackers be able to gain some knowledge about me? Or to track my activities? Or even worse, to steal my identity and impersonate me? All in all, how will biometric technology protect me? These and other questions commonly raise when dealing with Biometric solutions for security applications. This PhD Thesis is focused on the analysis of the security and privacy provided by biometric systems. More specifically, we will study the unlinkability and irreversibility of the templates stored in biometric databases and propose new biometric template protection schemes to ensure the privacy of the subject.

Over the last years, with the arrival of cloud computing and personal mobile devices in the so-called Digital Age, automatic person recognition has become a key factor in our everyday life. Not only we need to be identified to cross a border, but also to perform banking operations or even to unlock our smartphones. This has resulted in the establishment of a new technological area known as biometric recognition, or simply *biometrics* [Jain *et al.*, 2006]. The basic aim of biometrics is to discriminate automatically between subjects in a reliable way, and according to some target application, based on one or more signals derived from physical or behavioural characteristics, such as face, fingerprint, iris, voice, hand, signature, etc. These personal traits are commonly denoted as *biometric characteristics*.

Even if automatic person recognition has been a subject of study for more than forty years [Atal, 1976; Kanade, 1973], it has not been until the last decade when biometrics has been established as an specific research area. This is evidenced by recent reference texts [Jain *et al.*, 2011, 2008; Ratha and Govindaraju, 2008; Ross *et al.*, 2006; Tistarelli *et al.*, 2009], specific conferences [Bowyer *et al.*, 2015; Chellappa *et al.*, 2015; Fierrez *et al.*, 2013; Kittler *et al.*, 2014; Tistarelli and Maltoni, 2007; Vijaya-Kumar *et al.*, 2008], common benchmark tools and evaluations [Beveridge *et al.*, 2013; Cappelli *et al.*, 2006; LivDet, 2009; Mayoue *et al.*, 2009; Phillips *et al.*, 2000a; Phillips, 2006; Phillips *et al.*, 2011, 2009a,b; Przybocki and Martin, 2004; Yeung *et al.*, 2004], cooperative international projects [BBfor2, 2010; BioSec, 2004; Biosecure, 2007; COST, 2007; MTIT, 2009; TABULA RASA, 2010], international consortia dedicated specifically to biometric recognition [BC, 2009; BF, 2009; BI, 2009; EAB, 2012; EAB-CITeR, 2015; US

CITeR, 2011], standardization efforts [ANSI/NIST, 2009; BioAPI, 2009; ISO/IEC JTC 1/SC 27, 2009; ISO/IEC JTC 1/SC 37, 2009], and increasing attention both from government [BWG, 2009; DoD, 2009] and industry [IBIA, 2009; International Biometric Group, 2009].

Biometric technology presents several advantages over classical security methods based on something that you know (PIN, Password, etc.) or something that you have (key, card, etc.). These methods force the subject to remember difficult PIN codes, which could be easily forgotten, or to carry a key, which could be lost or stolen. Biometric recognition, on the other hand, is based on the very attractive principle that "you are your own key", which, therefore, cannot be lost or forgotten. Furthermore, traditional recognition systems cannot discriminate between impostors who have illegally acquired the privileges to access a system and the genuine subject, and cannot satisfy negative claims of identity (i.e., I am *not* John Doe) [Jain *et al.*, 2011].

For those reasons, some high-scale initiatives, such as the Indian Unique ID [Government of India, 2012] or the SmartBorders package [European Comission, 2013], have recently adopted biometrics as their recognition technology. Moreover, biometric systems have been recently introduced into the banking sector [European Association for Biometrics (EAB), 2015], reaching our smartphones through specific apps for particular banks[1], through general payments apps such as ApplePay or LoopPay, or even with Mastercard's "selfie" payments[2]. Furthermore, biometric ATMs[3,4] are currently being deployed.

However, in spite of those advantages, biometric systems present a number of drawbacks [Schneier, 1999], including the lack of secrecy (e.g., everybody knows our face or could get our fingerprints[5]), and the fact that a biometric characteristic cannot be replaced - if we forget a password we can easily generate a new one, but no new fingerprint can be generated if an impostor "steals" it. Recently, a database containing personal information of over five million federal US employees, including their fingerprints, was compromised[6]. Such a leakage will have a direct impact on these individuals' lives: among other consequences, affected employees may require "lifetime identity protection coverage".

It is thus of great importance for the definitive introduction of biometric systems in the security market to develop new template protection and privacy preserving methods which increase the security and privacy capabilities of this technology.

In order to prevent external attacks which can violate the privacy of the subjects [Adler, 2005; Hill, 2001; Matsumoto *et al.*, 2002; Venugopalan and Savvides, 2011], and increase the benefits of these systems for the enrolled subjects, biometric data should be protected. To that

[1] https://ingworld.ing.com/en/2014-4Q/7-ing-app

[2] http://www.cnet.com/news/mastercard-app-will-let-you-pay-for-things-with-a-selfie/

[3] http://www.biometricupdate.com/201301/citibank-launches-smart-atms-with-biometric-capabilities-in-asia

[4] http://www.biometricupdate.com/201508/ctbc-bank-piloting-atms-that-use-finger-vein-scanning-and-facial-recognition

[5] http://www.theregister.co.uk/2014/12/29/german_minister_fingered_as_hackers_steal_her_thumbprint_from_a_photo/

[6] http://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html

end, hashes [Kong *et al.*, 2006; Sutcu *et al.*, 2005; Teoh *et al.*, 2004], cryptographic techniques [Barni *et al.*, 2010; Luo *et al.*, 2009] or fuzzy extractors [Juels and Sudan, 2006; Juels and Wattenberg, 1999; Nandakumar and Jain, 2008] have been applied to biometric templates, at the cost of verification accuracy degradation in most cases.

Regarding the standardization of such protection techniques, while the International Organization for Standardization (ISO) published in 2009 an international standard on security evaluation of biometrics [ISO/IEC JTC1 SC27 IT Security Techniques, 2009], it has not been until the last years that efforts have been directed to the development of international standards for biometric template protection schemes [Rane, 2014]. Recently, the ISO has published the first standard on the protection of biometric information [ISO/IEC JTC1 SC27 IT Security Techniques, 2011], and is currently working on an international standard on template protection schemes testing [ISO/IEC JTC1 SC37 Biometrics, 2015].

In spite of those efforts, there is still a long way to go before a standardized methodology for the protection of biometric systems is defined and becomes extended practice as it occurs in other Information Technologies. This PhD Thesis pretends to bring some insight into the difficult problem of enhancing the security and privacy of biometric systems, proposing effective template protection schemes which can minimize the effects of potential attacks, in order to increase the confidence of the subjects in this thriving technology. This way, the experimental studies presented in this Dissertation can help to further develop the ongoing standardization efforts for the development of template protection schemes to improve the security and privacy of the systems.

1.1. Biometric Systems and Modalities

A biometric system is essentially a pattern recognition system which makes use of biometric characteristics to recognize individuals. As mentioned above, the objective is to establish an identity based on *who you are* or *what you produce*, rather than by *what you possess* or *what you know*. This paradigm not only provides enhanced security but also avoids, in recognition applications, the need to remember multiple passwords and maintain multiple authentication tokens. Who you are refers to *physiological* characteristics[1] such as face, iris or fingerprint. What you produce refers to *behavioural* patterns which entail a learning process and which characterize your identity, such as the gait, handwriting or the written signature.

The digital representation of the features of a biometric characteristic is known as *template*. Reference templates $\mathbf{T}_r$ are stored in the system database through the *enrolment* or *training* process, which is depicted in Figure 1.1 (left). The database can be either centralized (this is the case of most biometric systems working at the moment), or distributed (as in Match-on-Card systems where each subject carries the only copy of his template in a personal card [Bergman, 2008a]). Once the subjects have been enrolled to the system, the recognition process can be

[1] Although the term *physiological characteristic* is commonly used when describing biometrics, the purpose is to refer to the morphology of parts of the human body, therefore the proper term is *morphological characteristic*.

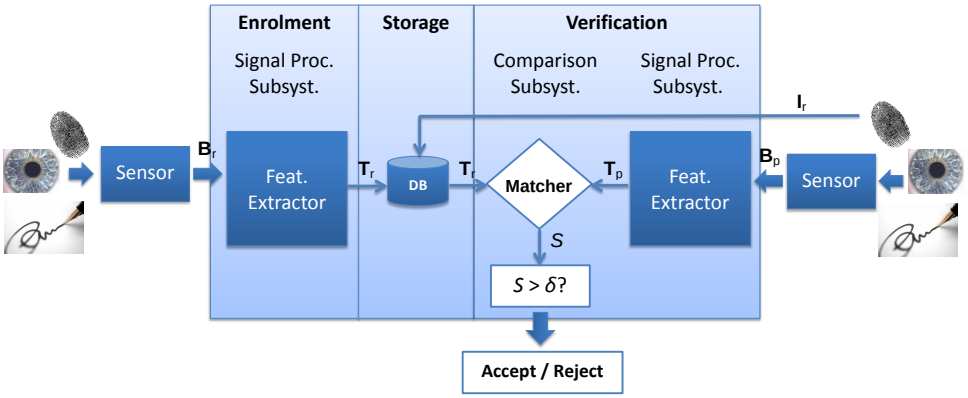


Figure 1.1: *Diagram of the two processes involved in a verification system: enrolment (left) and verification (right). Both processes occur at different points in time, being enrolment always prior to verification.*

performed in two modes [Jain *et al.*, 2011]:

- **Identification**. In this mode, the question posed to the system is: is this person in the database? The answer might be No (i.e., the person is unknown to the system), or any of the registered identities in the database. The system has thus to perform a one-to-many matching process, as it has to compare the input sample to all the stored templates.

  In most practical cases, under the identification operation mode, the system usually returns, in a ranked manner, those identities that are more likely to be the searched person in a previously created database (i.e., those that have produced a higher similarity score), and then a human expert decides whether the subject is or not within that reduced group of people. Typical identification applications include Automated Fingerprint Identification Systems [Komarinski, 2005].

- **Verification**. In this case, what we want to know is whether a person is really who she claims to be. Whereas the *impostors* can potentially be the world population, the *clients* or *targets* are known to the system through the enrolment process (Fig. 1.1 left). In this phase, reference templates $\mathbf{T}_r$ are extracted from the input biometric samples $\mathbf{B}_r$ and stored in the database.

  On the other hand, in order to authenticate a particular subject, the systems receives two inputs (Fig. 1.1 right): the probe biometric sample $\mathbf{B}_p$ and the claimed identity $\mathbf{I}_r$, corresponding to one of the templates previously stored in the database. The system performs a one-to-one matching process where the submitted biometric sample (more specifically, the template extracted from this probe sample, $\mathbf{T}_p$) is compared to the enrolled template $\mathbf{T}_r$ associated with the claimed identity, generating a score S. This score is subsequently compared to a pre-defined verification threshold δ in order to determine whether the subject is a *client* (the identity claim is *accepted*, $S > \delta$), or an *impostor* (the identity claim is *rejected*, $S < \delta$). Typical verification applications include network login, ATMs, physical access control, credit-card purchases, etc.

This Thesis is focused on the evaluation of biometric systems working under the verification mode. However, many of the algorithms and methods developed in the Thesis can be adapted in a straightforward manner to be used in identification systems.

As mentioned above, different biometric characteristics have been proposed and are used in various applications [Jain *et al.*, 2011]. In theory, any human characteristic can be used as a biometric identifier as long as it satisfies the following requirements:

- **Universality**, which indicates to what extent a biometric is present in the world population.
- **Distinctiveness**, which means that two persons should have sufficiently different biometrics.
- **Permanence**, which indicates that the biometric should have a compact representation invariant over a sufficiently large period of time.
- **Collectability**, which refers to the easiness of the acquisition process and to the ability to measure the biometric quantitatively.

Other criteria required for practical applications include:

- **Performance**, which refers to the efficiency, accuracy, speed, robustness and resource requirements of particular implementations based on the biometric.
- **Acceptability**, which refers to whether people are willing to use the biometric and in which terms.
- **Circumvention**, which reflects the difficulty to fool a system based on a given characteristic by fraudulent methods.

An ideal biometric system should meet all these requirements. Unfortunately, no single biometric characteristic satisfies all of them at the same time: while some biometrics have a very high distinctiveness (e.g., fingerprint or iris), they are relatively easy to circumvent (e.g., using a gummy finger, or an iris printed photograph). On the other hand, other biometrics such as vein patterns are very difficult to circumvent, but they are not easy to acquire. In order to compensate for those weaknesses, several characteristics can be combined in a single biometric system, known as *multi-biometric system* [Jain *et al.*, 2011]. Among other advantages of such multimodal biometric systems, verification accuracy increases, the recognition system becomes more robust to individual sensor or subsystem failures, and the number of cases where the system is not able to make a decision diminishes (e.g., bad quality biometric samples due to bad acquisition or deterioration).

1.2. Privacy Issues in Biometric Systems

While the use of biometric information for verification offers numerous advantages, many people are currently concerned about the possible misuse of biometric data [Bustard, 2015]. Among other concerns, biometric data could be used to reveal medical conditions, to gather personal information, even in a covertly manner given the recent developments in biometrics at a distance [Tistarelli *et al.*, 2009], or to link databases. Furthermore, geographical position, movements, habits and even personal beliefs can be tracked by observing when and where the biometric characteristics of an individual are used to identify him/her [Barni *et al.*, 2015].

In order to address those concerns, biometric data is considered *personal data* by the European Union data protection directive 95/46/EC [European Parliament, Oct. 1995.]: biometrics are an intrinsic part of the human body and/or behaviour, which we cannot discard in case of theft. Within this directive, *personal data* is defined as "*any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*". This means that *processing* of biometric data is subject to right of *privacy preservation*, where the notion of *processing* means "*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*". More recently, the EU Data Protection Reform IP/12/46 [European Parliament, 2012] raised biometric data to sensitive data, hence requiring a stronger privacy protection.

Those definitions imply that, in order to grant the subject's privacy, biometric information should be carefully protected both in its stored form (i.e., biometric templates or references) and any time it is used for verification purposes. In order to guarantee that privacy, we should pose ourselves several questions:

- *In the first place, do the stored templates reveal any information about the original biometric samples? In other words, are we able to reconstruct synthetic samples whose templates are similar enough to those of the original subject?* If such an inverse engineering process, also known as *inverse biometrics*, is possible, an eventual attacker which manages to obtain just a template belonging to a certain subject (e.g. the iriscode or minutiae template) would be able to reconstruct the original biometric sample. The attacker could afterwards use it to illegally access the system or even to steal someone's identity, thus violating the right of privacy preservation. As a consequence, we must ensure the *irreversibility* of the templates.

- *Even if templates were irreversible, are my enrolled templates in different recognition systems somehow related to each other? Can someone cross-match those templates and track my activities?* We should not only think about protecting the stored references in order to make infeasible the inverse biometrics process. With the widespread use of biometrics

in many everyday tasks, a particular subject will probably enrol in different applications, such as health care or on-line banking, with the same biometric instance (e.g., my right index finger). The right of privacy preservation also entails the right not to be tracked among those applications. If the answer to those questions is yes, we are facing an additional privacy issue: an eventual attacker who gets access to several templates enrolled in different systems could combine that information and further exploit it to gain knowledge of how many bank accounts we have or infer patterns in our regular activity. Therefore, *cross-matching* between templates used in different applications should be prevented.

- *Finally, what if someone steals a template extracted from my right index finger? Won't I be able to use that finger again to enrol into the system? Has it been permanently compromised?* Since biometric characteristics cannot be replaced, we should be able to generate multiple templates form a single biometric instance in order to discard and replace compromised templates. Furthermore, those templates should not be related to one another, in the sense that they should not be positively matched by the biometric system, to prevent the impersonation of a subject with a stolen template. Consequently, *renewability* of biometric templates is also desired. It should be noted that both cross-matching and renewability can be addressed at the same time if full *unlinkability* between templates belonging to the same subject is granted.

The relevance of these concerns and the efforts being directed to solve them within the biometric community are highlighted by some recent special issues in journals, such as the IEEE Signal Processing Magazine Special Issue on Biometrics Security and Privacy Protection [SPM, 2015], the development of international standards on biometric information protection, such as the ISO/IEC IS 24745 [ISO/IEC JTC1 SC27 IT Security Techniques, 2011], specific tracks on biometric security [Alonso-Fernandez and Bigun, 2016; Bowyer *et al.*, 2015] or privacy-enhancing technologies [Decker *et al.*, 2016; Locasto *et al.*, 2016] at international conferences, recent publications [Barni *et al.*, 2015; Ferrara *et al.*, 2014; Nandakumar and Jain, 2015; Rane, 2014] and PhD Thesis [Nagar, 2012; Sutcu, 2009; Zhou, 2012], or the EU FP7 project TURBINE on Trusted Revocable Biometrics Identities [TURBINE, 2007]. However, it is only since very recently that those concerns have been raised and started to be addressed.

This Dissertation analyses in a systematic manner the privacy offered by traditional biometric systems, showing the need for new approaches to biometric verification that ensure no sensitive personal data is leaked by either the verification process or the stored references. Furthermore, new protection algorithms are proposed to provide the required security and privacy to the subjects.

1.3. Biometric Template Protection

As a consequence of the privacy issues related to traditional biometric systems unveiled in Sect. 1.2, new standardization efforts are being currently directed to prevent such information

leakages. In particular, the ISO/IEC IS 24745 on biometric information protection [ISO/IEC JTC1 SC27 IT Security Techniques, 2011] encourages the substitution of traditional biometric systems (shown in Fig. 1.1) with biometric template protection schemes. This new approach involves a somehow different operation diagram, sketched in Fig. 1.2. The main differences with respect to the diagram shown in Fig. 1.1 are the following:

- At enrolment, the output of the Feature Extractor, the unprotected template $\mathbf{T}_r$, is not stored any more as reference in the database. A new module, the *Pseudonymous Identifier Encoder* (*PIE*), takes the template as input and generates the biometric reference, which now comprises two different pieces of information:
  - *Pseudonymous Identifier* (PI): this is the part of a renewable biometric reference that represents an individual within a certain domain by means of a protected identity (i.e., the protected equivalent to the unprotected template $\mathbf{T}_r$). At the time of verification, this is the element to be compared, possibly taking into account the Auxiliary Data (see below). It should be noted that the PI does not contain any information that allows retrieval of the original biometric sample, the original biometric features or the true identity of its owner.
  - *Auxiliary Data* (AD): subject-dependent data that is part of a renewable biometric reference and may be required to reconstruct pseudonymous identifiers during verification.

  Both parts may be stored in different databases, as depicted in Fig. 1.2 (center).
- Similarly, at verification time, the classical probe template $\mathbf{T}_p$ (see Fig. 1.2 right) is discarded and substituted by the output of a new module called *Pseudonymous Identifier Recorder* (*PIR*), which takes as input the probe template $\mathbf{T}_p$ and the stored AD_r (if any), and computes the PI_p of the acquired sample.
- Finally, the *Pseudonymous Identifier Comparator* (*PIC*) will output a similarity score S between the reference protected template, PI_r, corresponding to the identity claimed, $\mathbf{I}_r$, and the probe protected template, PI_p. As in traditional biometric systems, S is compared to the verification threshold δ to reach the final verification decision.

To sum up, in biometric template protection schemes, unprotected templates ($\mathbf{T}_p$, $\mathbf{T}_r$) are neither stored in the database nor compared for verification purposes. New modules are added to the system (*PIE*, *PIC* and *PIR*), which extract and compare renewable and protected references (PI_p, PI_r). In case of leakage, those references disclose no biometric information about the subjects, thus protecting the privacy of the subjects. In the rest of the Dissertation, unprotected templates will be denoted as $\mathbf{T}$ and their protected counterparts as $\mathbf{C}$.

In order to guarantee this privacy, in accordance with the ISO/IEC IS 24745 [ISO/IEC JTC1 SC27 IT Security Techniques, 2011], biometric template protection schemes have to comply with the two major requirements of *irreversibility* and *unlinkability*:

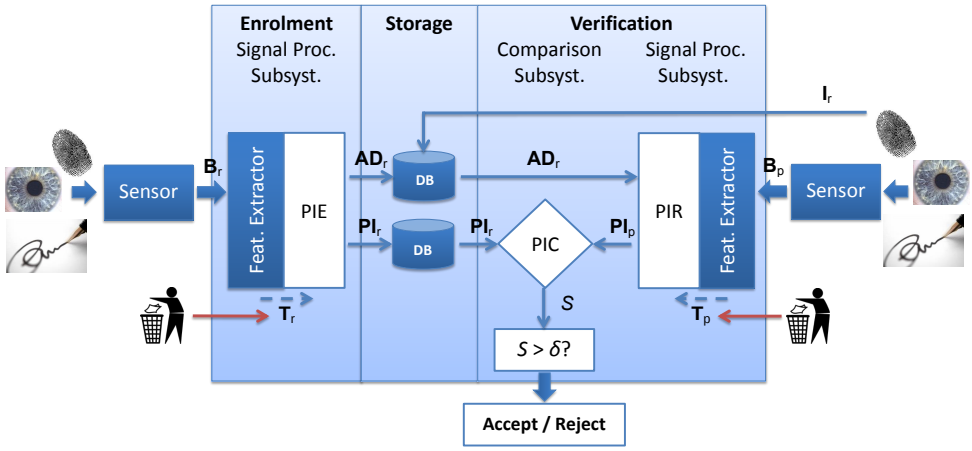


Figure 1.2: *Diagram of the two modes of operation in a Biometric Template Protection system: enrolment (left) and verification (right). Both processes occur at different points in time, being enrolment always prior to verification. PIE stands for Pseudonymous Identifier Encoder, PIC for Pseudonymous Identifier Comparator, PIR for Pseudonymous Identifier Recorder and AD for Auxiliary Data.*

- *Irreversibility*: in order to overcome the first privacy issue described in the previous section (i.e., amount of biometric information which is leaked by the template), we require that knowledge of a protected template $\mathbf{C}$ and corresponding auxiliary data AD cannot be exploited to reconstruct a biometric signal $\mathbf{B}'$ which positively matches the original biometric sample $\mathbf{B}$. This property prevents the abuse of stored biometric data for launching spoof or replay attacks, thereby improving the security of biometric systems [Nandakumar and Jain, 2015].

- *Unlinkability*: in order to overcome the second and third aforementioned drawbacks of unprotected verification systems (i.e., biometric characteristics should not be matched across systems and they should be replaceable), given a single biometric sample $\mathbf{B}$, it must be feasible to generate different versions of protected templates $\mathbf{C}^1, \mathbf{C}^2, \ldots, \mathbf{C}^n$, so that those templates cannot be linked to a single subject. This property guarantees the privacy of a subject when he is registered in different applications with the same biometric instance (prevents cross-matching), and also allows issuing new credentials in case a protected template is stolen.

In addition to the irreversibility and unlinkability properties, biometric template protection approaches should not affect other important performance parameters of conventional biometric recognition systems [Simoens *et al.*, 2012b]. For instance, *accuracy* of unprotected systems should be preserved and *verification speed* should be comparable in order to enable real-time verification.

Even if the research community has dedicated serious efforts to the proposal and development of new biometric template protection schemes [Patel *et al.*, 2015; Rathgeb and Uhl, 2011],

some commercial schemes such as BioHASH[1] are being distributed, and some standardization efforts are currently being made [ISO/IEC JTC1 SC37 Biometrics, 2015; Rane, 2014], third-party standardized evaluation of the revocable methods is still needed. To that end, two main approaches may be adopted: *security through obscurity* or *security through transparency* (also known as *security by design*). The security through transparency scheme follows Kerckhoffs' principle [Kerckhoffs, 1883]: a cryptosystem should be secure even if everything about the system, except the key, is public knowledge. This principle can be applied to any security related technology, in particular biometrics: in words of the Biometric Working Group [BWG, 2009], in the context of biometric recognition, applying security through transparency would mean to "*make public exposure of countermeasures and vulnerabilities which will lead to a more mature and responsible attitude from the biometrics community and promote the development of more secure systems in the future*" [BWG, 2003].

We believe that exposing foreseeable threats, evaluating biometric systems vulnerabilities to those threats, and proposing new biometric template schemes and/or countermeasures, is the path that leads to a stronger and more robust biometric technology. This way, throughout the Dissertation different threats that may compromise the privacy granted by biometric systems are pointed out, systematically evaluated, and new biometric template protection schemes which can guarantee a higher level of security and privacy to the subject are proposed. In other words, this Thesis pretends to shed some light into the privacy and security evaluation of biometric systems, not only proposing new biometric template protection schemes but also contributing to the development of some guidelines and procedures for standardized evaluation and testing, "*a necessary step to enable vendors to test their offerings, compare their performance against competitors, offer end-to-end solutions, and make large-scale deployment of biometric template protection schemes a reality*", as stated by Rane [2014].

1.4. Motivation of the Thesis

Provided that biometrics is a very powerful tool for reliable automatic identity verification and that, as presented in the previous sections, security and privacy evaluation is a key issue for the acceptance of any security-based technology among the enrolled subjects, this Thesis is focused on the security and privacy assessment of biometric systems and the proposal of new and general biometric template protection schemes to counterfeit the exposed privacy threats. The research carried out in this area has been mainly motivated by four observations from the state-of-the-art.

First, in line with the *security through transparency* security principle [Kerckhoffs, 1883], to assess the privacy granted by biometric template protection systems, we need to identify the threat in order to later quantify the danger posed. This leads to a constant need to search for new weak points in security applications, in order to make them public and motivate both industry and researchers to look for solutions to the threat. This is the only way to provide

[1] `http://www.genkey.com/en/technology/biohashr-sdk`

appropriate countermeasures and ensure the full privacy protection that the enrolled subjects require.

In the second place, the development of new biometric template protection schemes which fulfil all the requirements established by the ISO/IEC IS 24745 standard on biometric information protection [ISO/IEC JTC1 SC27 IT Security Techniques, 2011], is currently a research challenge (we refer the reader to Chapter 2 for a review of the current state-of-the-art in the field). Although different efforts have been carried out in this direction [Ratha *et al.*, 2001; Sutcu *et al.*, 2005], there is still no definitive solution: even if irreversible and unlinkable schemes have been proposed, there is a significant gap between the unprotected systems and their protected counterparts in terms of verification accuracy [Nandakumar and Jain, 2015]. There is a hence need for new protection methods that comply with the ISO requirements, even under challenging adversary models [Simoens *et al.*, 2012a].

There is also a lack of protection schemes that can be applied to different biometric characteristics. Most of the current biometric template protection schemes are designed specifically for one biometric characteristic [Nandakumar *et al.*, 2007; Pillai *et al.*, 2011], and cannot be extended to other modalities in a straightforward manner. As a consequence, new methodologies to protect the systems, applicable to any given biometric modality, should be designed in order to achieve fully unlinkable and irreversible biometric systems.

Last but not least, the fourth observation is strongly related to the previous ones. In the existing publications, experimental results are obtained and reported without following any general or systematic protocol, not taking into account all necessary aspects of a rigorous security and privacy assessment (not only should we analyse whether a zero effort attack can be performed to extract biometric information from the templates, but also analyse attacks designed *ad hoc* for a particular biometric template protection scheme). Moreover, in many cases only proprietary databases are used. As a consequence, the reported results cannot be compared, losing this way part of their utility, in accordance with *reproducible research* principles [Fomel and Claerbout, 2009; Peng, 2011; Vandewalle *et al.*, 2009].

1.5. The Thesis

The Thesis developed in this Dissertation can be stated as follows:

In order to facilitate the wide deployment of biometric systems in real-time scenarios, templates need to be protected in a standardized manner, preserving the privacy of the subject from inverse biometrics and cross-matching attacks so that irreversibility and unlinkability are granted. At the same time, verification accuracy, template size and verification speed should be maintained with respect to their unprotected counterparts.

Given the Thesis stated above, the main objectives pursued are as follows:

- Reviewing and studying the problem of security and privacy assessment in biometric systems in order to identify and evaluate new possible threats.
- Devising new practical biometric template protection schemes to counterfeit the analysed privacy issues, in order to enhance the robustness of biometric systems to attacks.
- Applying the proposed techniques and methodologies to common scenarios, systems, and databases widely available for the biometrics research community, with emphasis on face, signature, iris, handshape, fingervein and fingerprint verification systems.

In order to reach the previous objectives, in this PhD Thesis we follow a two-step approach: *i*) commonly used unprotected templates are evaluated and proved to be reversible, and *ii*) new general methods are proposed in order to add irreversibility, unlinkability and robustness to cross-matching attacks to the original unprotected biometric systems. Even though most security and privacy evaluations of template protection schemes focus only on the analysis of the similarity scores provided by the system [Rathgeb and Uhl, 2011], a more thorough evaluation should be carried out, taking into account cross-matching attacks specifically designed for the scheme at hand, and considering challenging adversary models where the attacker is in possession of protected templates and any secret information used at verification time [Simoens *et al.*, 2012a].

1.6. Outline of the Dissertation

The Dissertation is structured according to a traditional complex type with background theory, practical methods, and three independent experimental studies in which the methods are applied [Paltridge, 2002]. The chapter structure is as follows:

- Chapter 1 introduces the topic of privacy and security in biometric systems, and gives the motivation, objectives, outline and contributions of this PhD Thesis.
- Chapter 2 summarizes related works on which this Thesis is motivated.
- Chapter 3 (background theory) considers the issue of privacy preservation in biometric systems and presents the common methodology followed in the Dissertation for the accuracy, security and privacy evaluation of unprotected and protected biometric systems. In particular, a new framework for templates' unlinkability analysis is proposed. The biometric databases and unprotected systems used in this Dissertation are also described.
- Chapter 4 (experimental) introduces two novel methods for the reconstruction of biometric samples from the templates stored in the database: *i*) an inverse biometrics method based on the uphill simplex algorithm and a biometric samples generator, and *ii*) an inverse biometrics method based on genetic algorithms. These methods are then used to evaluate the irreversibility of a handshape- and an iris-based verification systems.

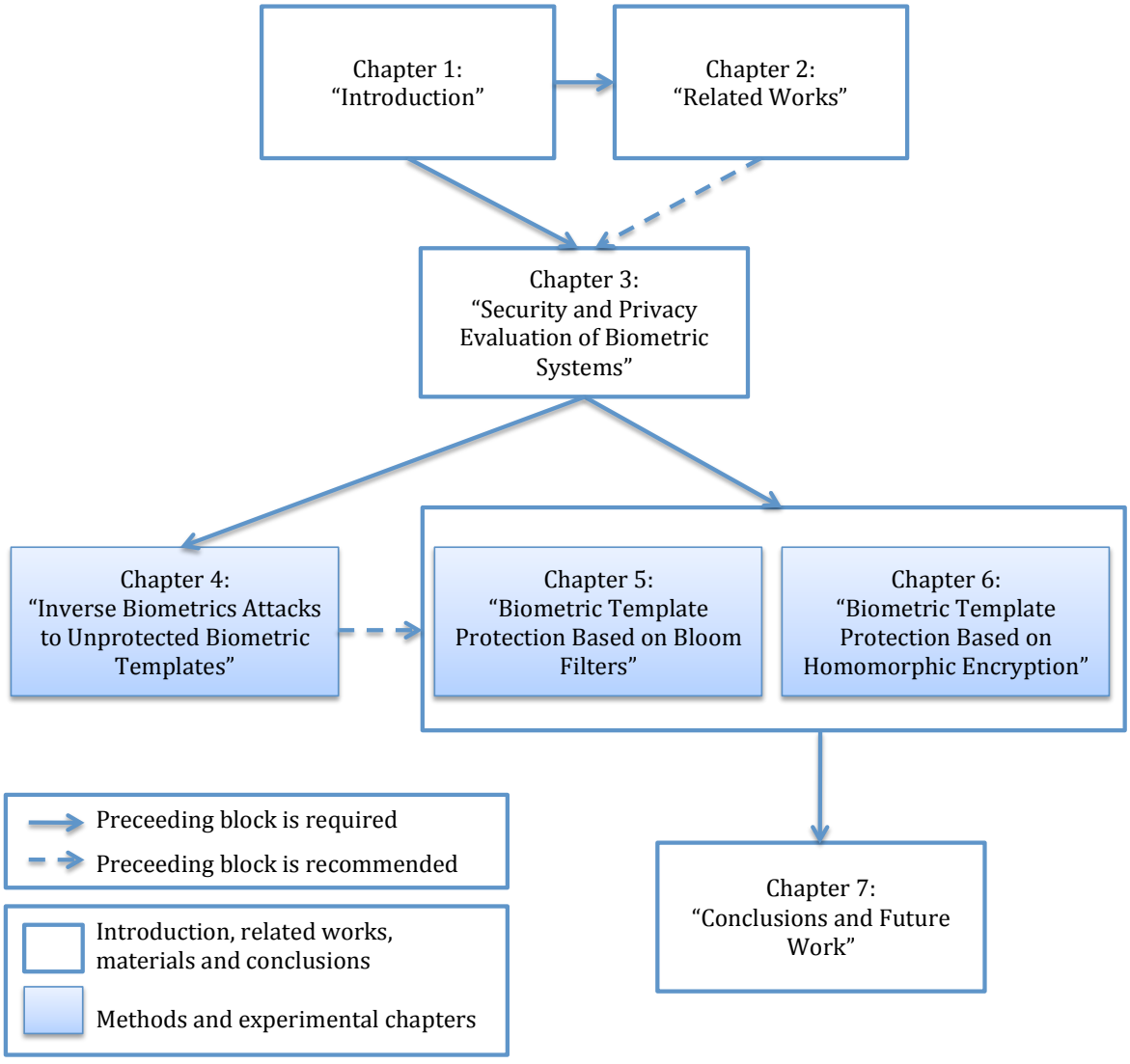


Figure 1.3: *Dependence among Dissertation chapters.*

- Chapter 5 (experimental) introduces a novel biometric template protection scheme based on Bloom filters in a stepwise manner: *i*) the original scheme, providing irreversibility, is first described, *ii*) then a structure-preserving feature re-arrangement of the unprotected features is proposed in order to add unlinkability to the original system, *iii*) a protocol for estimating the appropriate values for the system parameters is then devised, and *iv*) a general weighted feature level fusion for Bloom filter based templates is finally presented. In the experimental evaluation, the soundness of the parameter estimation method is analysed and the accuracy, irreversibility, unlinkability and robustness to cross-matching attacks of the scheme are assessed, for iris-, face-, fingerprint- and fingervein-based biometric systems.

- Chapter 6 (experimental) introduces three novel methods for the application of Homomorphic Encryption (HE) to biometric template protection systems: *i*) a scheme for the comparison of templates of variable-length based on Dynamic Time Warping and HE, *ii*) a general scheme for the application of HE to the comparison of fixed-length templates with the Mahalanobis distance, the Euclidean distance and the Cosine similarity, and *iii*) a general framework for feature, score and decision level fusion within biometric template protection systems based on HE. The proposed methods are evaluated on on-line signature and fingerprint based biometric systems, analysing the verification accuracy, the irreversibility and the unlinkability provided, as well as the computational complexity.

- Chapter 7 concludes the Dissertation summarizing the main results obtained and outlining future research lines.

The dependence among the chapters is illustrated in Fig. 1.3. For example, reading Chapter 3 is required before reading any of the experimental Chapters 4, 5 and 6 (shaded in Fig. 1.3). Before Chapter 3 one should start with the introduction in Chapter 1, and the recommendation of reading Chapter 2. Following the guidelines given in Fig. 1.3 and assuming a background in biometrics [Jain *et al.*, 2011], one can optionally read the experimental Chapter 4 before Chapters 5 and 6, which in turn can be read independently.

The methods developed in this PhD Thesis are strongly based on popular approaches from the pattern recognition literature. The reader is referred to standard texts for a background on the topic [Duda *et al.*, 2001; Theodoridis and Koutroumbas, 2008]. This is especially useful for dealing with Chapter 4. Chapters 4 to 6 also assume a knowledge of the fundamentals of image processing [Gonzalez and Woods, 2006], and pattern recognition [Bigun, 2006]. Finally, Chapter 6 assumes some knowledge of public key cryptography [Ferguson and Schneier, 2003; Goldwasser and Micali, 1984] and Homomorphic Encryption [Fontaine and Galand, 2007].

1.7. Detailed Research Contributions

The research contributions of this PhD Thesis are the following (for clarity, journal papers included in ISI JCR appear in bold):

- NOVEL INVERSE BIOMETRICS ATTACKS.

  1. Novel inverse biometrics method based on the Uphill simplex algorithm

     - M. Gomez-Barrero, J. Galbally, A. Morales, M. A. Ferrer, J. Fierrez and J. Ortega-Garcia, "Inverse Biometrics: A Case Study in Hand Geometry Authentication", in *Proc. IAPR Int. Conf. on Pattern Recognition (ICPR)*, pp. 1281-1284, Tsukuba, Japan, November 2012.
     - **M. Gomez-Barrero, J. Galbally, A. Morales, M. A. Ferrer, J. Fierrez and J. Ortega-Garcia, "A novel hand reconstruction approach and its application to vulnerability assessment", *Information Sciences*, Vol. 268, n. 0, pp. 103-121, June 2014.**

  2. Novel inverse biometrics method based on genetic algorithms.

     - **J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez and J. Ortega-Garcia, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms", *Computer Vision and Image Understanding*, Vol. 117, n. 10, pp. 1512-1525, October 2013 (Selected for Elsevier Virtual Issue: Celebrating the Breadth of Biometrics Research).**

- NEW BIOMETRIC TEMPLATE PROTECTION SYSTEMS.

  1. Novel biometric template protection scheme based on Bloom filters for facial features.

     - M. Gomez-Barrero, C. Rathgeb, J. Galbally, J. Fierrez and C. Busch, "Protected Facial Biometric Templates Based on Local Gabor Patterns and Adaptive Bloom Filters", in *Proc. IAPR/IEEE Int. Conf. on Pattern Recognition (ICPR)*, pp. 4483-4488, Stockholm, Sweden, August 2014.

  2. Novel multi-biometric template protection scheme based on Bloom filters for facial and iris features.

     - C. Rathgeb, M. Gomez-Barrero, C. Busch, J. Galbally and J. Fierrez, "Towards Cancelable Multi-Biometrics based on Adaptive Bloom Filters: A Case Study on Feature Level Fusion of Face and Iris", in *Proc. Int. Workshop on Biometrics and Forensics (IWBF)*, Gjøvik, Norway, March 2015a.

  3. Novel general biometric and multi-biometric template protection scheme based on Bloom filters complying to high standards with the requirements of the ISO/IEC IS 24745 on biometric information protection:

     - **M. Gomez-Barrero, C. Rathgeb, J. Galbally, C. Busch and J. Fierrez, "Unlinkable and Irreversible Biometric Template Protection Based on Bloom Filters", *Information Sciences*, 2016 (Submitted).**
     - **M. Gomez-Barrero, C. Rathgeb, G. Li, R. Ramachandra, J. Galbally and C. Busch, "General Framework for Multi-Biometric Template Protection Based on Bloom Filters", in *Information Fusion*, 2016 (Submitted).**

4. Novel biometric template protection schemes based on Homomorphic Encryption for unimodal systems.

   - M. Gomez-Barrero, J. Galbally and J. Fierrez, "Variable-Length Template Protection Based on Homomorphic Encryption with Application to Signature Biometrics", in *Proc. Int. Workshop on Biometrics and Forensics (IWBF)*, Limassol, Cyprus, March 2016.
   - M. Gomez-Barrero, J. Galbally, E. Maiorana, P. Campisi and J. Fierrez, "Fixed-Length Template Protection Based on Homomorphic Encryption with Application to Signature Biometrics", in *Proc. Int. Conf. on Computer Vision and Pattern Recognition*, Las Vegas, USA, June 2016 (Submitted).

5. Novel multi-biometric template protection scheme based on Homomorphic Encryption.

   - **M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi and J. Fierrez, "Multibiometric Template Protection Based on Homomorphic Encryption. A Case Study on On-Line Signature and Fingerprint", *IEEE Trans. on Information Forensics and Security*, 2016 (Submitted).**

- LITERATURE SURVEYS.

1. Privacy issues in biometric systems.

   - M. Gomez-Barrero and J. Gabally, "Inverse Biometrics and Privacy", C. Vielhauer (Eds.), *User-Centric Privacy and Security in Biometrics*, IET (to appear).

Other contributions related to the problem developed in this Thesis but not presented in this Dissertation include:

- NOVEL BIOMETRIC ATTACKS.

1. Novel hill-climbing attack based on the Uphill Simplex.

   - M. Gomez-Barrero, J. Galbally, J. Fierrez and J. Ortega-Garcia, "Hill-Climbing Attack Based on the Uphill Simplex Algorithm and its Application to Signature Verification", in *Proc. European Workshop on Biometrics and Identity Management (BioID)*, Springer LNCS-6583, pp. 83-94, Brandenburg, Germany, March 2011.
   - M. Gomez-Barrero, J. Galbally, J. Fierrez and J. Ortega-Garcia, "Face verification put to test: a hill-climbing attack based on the uphill-simplex algorithm", in *Proc. Intl. Conf. on Biometrics (ICB)*, pp. 40-45, New Delhi, India, March 2012.
   - M. Gomez-Barrero, J. Gonzalez-Dominguez, J. Galbally and J. Gonzalez-Rodriguez, "Security Evaluation of i-Vector Based Speaker Verification Systems Against Hill-Climbing Attacks", in *Proc. Conf. of the Int. Speech Communication Association (InterSpeech)*, pp. 935-939, Lyon, France, August 2013.

2. Novel hill-climbing attack based on genetic algorithms.

   - M. Gomez-Barrero, J. Galbally, P. Tome and J. Fierrez, "On the Vulnerability of Iris-based Systems to a Software Attack based on a Genetic Algorithm", in *Proc. Iberoamerican Conference on Pattern Recognition (CIARP)*, Springer LNCS-7441, pp. 114-121, Buenos Aires, Argentina, September 2012.

3. Novel hill-climbing attack to multi-biometric systems.

   - M. Gomez-Barrero, J. Galbally, J. Fierrez and J. Ortega-Garcia, "Multimodal Biometric Fusion: a Study on Vulnerabilities to Indirect Attacks", in *Proc. Iberoamerican Congress on Pattern Recognition (CIARP)*, Springer LNCS-8259, pp. 358-365, La Habana, Cuba, November 2013.
   - **M. Gomez-Barrero, J. Galbally and J. Fierrez, "Efficient software attack to multimodal biometric systems and its application to face and iris fusion", *Pattern Recognition Letters*, Vol. 36, pp. 243-253, January 2014.**

- LITERATURE SURVEYS.

  1. Attacks and countermeasures in biometric systems.

     - J. Galbally and M. Gomez-Barrero, "A Review of Iris Anti-Spoofing", in *Proc. Int. Workshop on Biometrics and Forensics (IWBF)*, Limassol, Cyprus, March 2016.
     - M. Gomez-Barrero and J. Gabally, "Software Attacks on Iris Recognition Systems", C. Busch and C. Rathgeb (Eds.), *Iris and Periocular Biometrics*, IET (to appear).
     - J. Galbally and M. Gomez-Barrero, "Presentation Attack Detection in Iris Recognition", C. Busch and C. Rathgeb (Eds.), *Iris and Periocular Biometrics*, IET (to appear).

- NOVEL BIOMETRIC SYSTEMS.

  1. Novel on-line signature recognition based on real on-line data and synthetic off-line data.

     - **J. Galbally, M. Diaz-Cabrera, M. A. Ferrer, M. Gomez-Barrero, A. Morales and J. Fierrez, "On-Line Signature Recognition Through the Combination of Real Dynamic Data and Synthetically Generated Static Data", *Pattern Recognition*, Vol. 48, pp. 2921-2934, September 2015.**

  2. Improved on-line signature verification system based on forgeries detection.

     - M. Gomez-Barrero, J. Galbally, J. Fierrez, J. Ortega-Garcia and R. Plamondon, "Enhanced On-Line Signature Verification Based on Skilled Forgery Detection Using Sigma-LogNormal Features", in *Proc. IEEE/IAPR Int. Conf. on Biometrics (ICB)*, pp. 501-506, Phuket, Thailand, May 2015. (**Siew-Sngiem Best Paper Award at ICB 2015**)

  3. New synthetic off-line signature generation based on real on-line data.

     - M. A. Ferrer, J. Galbally, M. Diaz-Cabrera, A. Morales and M. Gomez-Barrero, "Realistic Synthetic Off-line signature Generation Based on Synthetic On-line Data", in *Proc. IEEE Int. Carnahan Conf. on Security Technology (ICCST)*, pp. 116-121, Medellin, Colombia, October 2013.
     - M. Diaz-Cabrera, M. Gomez-Barrero, A. Morales, M. A. Ferrer and J. Galbally, "Generation of Enhanced Synthetic Off-line Signatures Based on Real On-line Data", in *Proc. IAPR Int. Conf. on Frontiers in Handwriting Recognition (ICFHR)*, pp. 482-487, Crete, Greece, September 2014.

- OTHER CONTRIBUTIONS TO BIOMETRIC TEMPLATE PROTECTION.

  1. Novel biometric template protection scheme based on Bloom filters and Honey Templates.

     - **E. Martiri, M. Gomez-Barrero, B. Yang and C. Busch, "Biometric Template Protection Based on Bloom Filters and Honey Templates", *IET Biometrics*, 2016 (Submitted).**

- OTHER NEW EXPERIMENTAL STUDIES.

  1. Effects of ageing on Sigma-Lognormal features for on-line signature.

     - M. Gomez-Barrero, J. Galbally, R. Plamondon, J. Fierrez and J. Ortega-Garcia, "Variations of Handwritten Signatures with Time: A Sigma-Lognormal Analysis", in *Proc. IEEE/IAPR Int. Conf. on Biometrics (ICB)*, Madrid, Spain, June 2013. (**Best Voted Poster Paper Award at ICB 2013**)

  2. Protection scheme for automatic iris recognition systems against masquerade attacks carried out with synthetically reconstructed iris images.

     - J. Galbally, M. Gomez-Barrero, A. Ross, J. Fierrez and J. Ortega-Garcia, "Securing iris recognition systems against masquerade attacks", in *Proc. SPIE Biometric and Surveillance Technology for Human and Activity Identification X, BSTHAI*, Vol. 8712, pp. 87120E, Baltimore, USA, May 2013.

  3. Organization of the first keystroke biometrics ongoing competition.

     - A. Morales, J. Fierrez, M. Gomez-Barrero and J. Ortega-Garcia, "KBOC: Keystroke Biometrics OnGoing Competition", in *Proc. IEEE Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS)*, Niagara Falls, USA, September 2016 (to appear).

Chapter 2

Related Works

This chapter summarizes previous works related to this PhD Thesis. We have focused on the two fields within biometrics research in which novel contributions have been made, namely: *i*) inverse biometrics methods to recover samples from stored templates, and *ii*) biometric template protection schemes. The aim of this chapter is not to generate a comprehensive and exhaustive review of the existing publications dealing with each of the aforementioned topics, but to summarise the most relevant works closely related to this Thesis, and which can help the reader to compose a general view of the state of the art on each of the matters.

The chapter is structured as follows. First we give an overview of the most important works on synthetic biometric samples generation, and, more specifically, on inverse biometrics (Sect. 2.1). Sect. 2.2 then focuses on the most important contributions existing in the state-of-the-art to Biometric Template Protection for unimodal systems, as a countermeasure to the issues raised in the previous section. Then Sect. 2.3 focuses on Multi-Biometric Template Protection. Finally the summary and conclusions of the chapter are presented (Sect. 2.4).

This chapter is based on the publications: [Galbally *et al.*, 2013; Gomez-Barrero *et al.*, 2014b, 2016c,e; Rathgeb and Uhl, 2011].

2.1. Inverse Biometrics

A growing interest has arisen in the biometric community over the last decade for *synthetic biometric samples generation* for different biometric characteristics, such as voice [Dutoit, 2001], fingerprints [Cappelli, 2003], iris [Cui *et al.*, 2004; Makthal and Ross, 2005; Shah and Ross, 2006; Wei *et al.*, 2008; Zuo *et al.*, 2007], handwriting [Lin and Wang, 2007], face [Poh *et al.*, 2003] or signature [Galbally *et al.*, 2012a,b; Popel, 2007]. The main reason behind that interest is the wide range of applications of those synthetic samples, which include but are not limited to:

- Increase of biometric data: the amount of available data belonging to the enrolled subjects could be augmented with synthetic samples. This way, verification accuracy could be improved, especially for modalities such as the signature where the intra-class variability

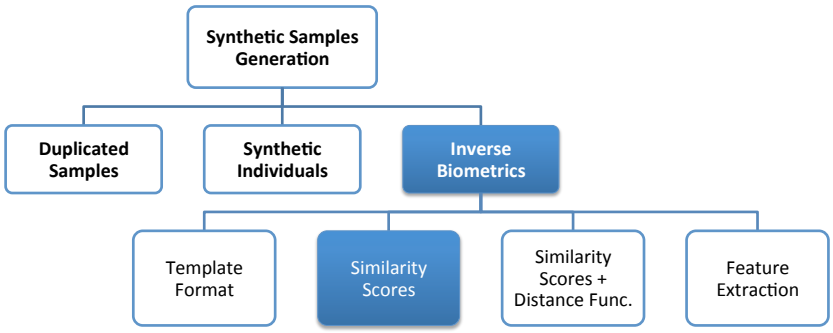


Figure 2.1: *Classification of the methods for synthetic biometric samples generation. Inverse biometrics methods are classified according to the knowledge required to be carried out. The categories to which the methods proposed in the Dissertation belong are highlighted in blue.*

is large [Fierrez and Ortega-Garcia, 2008; Galbally *et al.*, 2015, 2009].

- Generation of completely synthetic databases: due to the legal restrictions regarding data protection and the sharing and distribution of biometric data among different research groups, we can use synthetic databases to overcome the usual shortage of large biometric databases, with no privacy concerns since data does not belong to real subjects. Furthermore, this databases have no size restrictions, in terms of number of subjects and samples per subject, since they are automatically produced by a computer.

- Pseudo-identities generation: enrolled templates could be substituted by synthetic templates generated from reconstructed samples, thereby protecting the privacy of the subjects [Othman and Ross, 2013].

- Vulnerability and irreversibility studies: an attacker could use synthetically reconstructed images, which would be positively matched to the stored reference, to impersonate the enrolled subjects [Venugopalan and Savvides, 2011]. Furthermore, the irreversibility of the stored templates can be analysed in terms of whether it is possible to reconstruct such synthetic samples.

Depending on the final purpose, different types of synthetic data might be created. Therefore, synthetic sample generation methods can be broadly divided into three categories, as depicted in Fig. 2.1:

- **Duplicated samples**: in these methods the generation algorithm starts from one or more real samples of a given person and, through different transformations, produces different synthetic (or duplicated) samples corresponding to the same subject. This approach has been applied to signature [Munich and Perona, 2003; Oliveira *et al.*, 1997], handwriting [Mori *et al.*, 2000; Wang *et al.*, 2002] or face synthesis [Poh *et al.*, 2003; Wang and Zhang, 2004; Wilson *et al.*, 2002].

- **Synthetic individuals**: in this case, some kind of a priori knowledge about a certain biometric characteristic (e.g., minutiae distribution, iris structure, signature length, etc.)

is used to create a model of the biometric characteristic for a population of subjects. New synthetic individuals can then be generated sampling the constructed model. In a subsequent stage of the algorithm, multiple samples of the synthetic subjects can be generated by any of the procedures for creating duplicated samples. Different model-based algorithms have been presented in the literature to generate synthetic individuals for biometric characteristics such as iris [Cui *et al.*, 2004; Shah and Ross, 2006; Zuo *et al.*, 2007], fingerprint [Cappelli, 2003], speech [Klatt, 1980; Pinto *et al.*, 1989] or signature [Galbally *et al.*, 2012a].

- **Inverse biometrics**: in these methods, given a genuine template, the aim is the reconstruction of a synthetic biometric sample, which matches the stored biometric reference according to a particular biometric recognition system. In other words, it denotes a reverse engineering process which reconstructs synthetic samples from the information conveyed in real biometric templates, and which has already been applied to fingerprint [Cappelli *et al.*, 2007; Hill, 2001], iris [Venugopalan and Savvides, 2011] and face [Adler, 2003].

The first type of methods (i.e., duplicated samples) poses no additional privacy threats to the enrolled subjects: in order to generate synthetic samples, the potential attacker is already in possession of real biometric data belonging to the same subject. Similarly, the generation of fully synthetic individuals raises no privacy concerns, as no biometric information belonging to real subjects is derived. On the other hand, inverse biometric methods do result in a potential violation of the subject's privacy: given only a theoretically secure representation of the subject's biometric characteristics (i.e., the unprotected template), sensible biometric information can be obtained. In addition, contrary to the common belief that templates do not comprise enough information in order to reconstruct the original sample from them [International Biometric Group, 2002], synthetic samples can be generated and used to impersonate a particular subject, launching masquerade attacks. Since the main aim of the Dissertation is the analysis and improvement of the security and privacy provided by biometric systems, we will focus in the following on this last approach, as highlighted in Fig. 2.1, where inverse biometric methods are further classified in terms of the knowledge required to be carried out. In addition, a summary of the inverse biometrics methods introduced in the literature is shown in Table 2.1.

One of the first works that addressed the problem posed by inverse biometrics was carried out by Hill [2001]. He proposed a general scheme for the reconstruction of biometric samples, consisting in four successive steps, where only access and knowledge of the **templates format** stored in the database is required. In the first step, the attacker needs to gain access to one or more biometric templates. Then, he or she needs to understand the structure of the template (i.e., what information is stored, which format is used, etc.). After fully determining the structure of the templates, a reverse engineering process is carried out in order to reconstruct one or more *digital* biometric samples. Finally, the eventual attacker could also reconstruct *physical* artefacts from the digital synthetic samples.

The most challenging step is the third one, that is, devising a method for reconstructing

Table 2.1: *Summary of key inverse biometric approaches.*

Characteristic	Knowledge	Reference	Acceptance Rate	Database
Fingerprint	Template Format	Hill [2001]	100%	FVC2000 (110 subjects)
		Cappelli *et al.* [2007]	> 90% 0.1% FMR	FVC2002-DB1 (110 subjects)
		Galbally *et al.* [2010a]	> 99% 0.1% FMR	FVC2006 (140 subjects)
		Ross *et al.* [2007]	> 23% Rank 1	NIST-4f
Face	Simmilarity Scores	Adler [2003]	-	FRS
		Adler [2004]	> 95% 1% FMR	NIST Mugshot (110 subjects)
		Galbally *et al.* [2010b]	99-100% 0.1% FMR	XM2VTS (295 subjects)
	Distance Function	Mohanty *et al.* [2007]	> 72% 1% FMR	FERET (1196 subjects)
Iris	Feature Extraction	Venugopalan and Savvides [2011]	> 96% 0.1% FMR	NIST ICE 2005 (132 subjects)

digital samples given only the stored templates. In [Hill, 2001], a particular case study on minutiae-based fingerprint templates is presented, based on three consecutive steps: *i*) fingerprint shape estimation, *ii*) orientation field creation and *iii*) ridge pattern synthesis. In the first step, decision trees or neural networks are used, depending on the information available in the template. The orientation field creation relies on the singular points. In the final step, the ridge pattern is iteratively synthesised starting on the minutiae positions and guided by the orientation field.

A similar approach for the generation of fingerprint samples from standard minutiae-based fingerprint templates [ISO/IEC JTC1 SC 37 Biometrics, 2011] was proposed in [Cappelli *et al.*, 2007]. The fingerprint area is estimated with a greedy heuristic algorithm, based on the available minutiae positions. The Nelder-Mead simplex algorithm [Nelder and Mead, 1965] is used to synthesise the orientation map, which is used together with the set of minutiae and a fixed frequency to estimate the ridge pattern. In contrast to Hill's approach, using different frequency values on this last step, different synthetic samples can be obtained from a single template. Finally, an additional rendering step is carried out, in which noise is added to the "perfect" reconstructed image, thus yielding more realistic images, which in around 90% of the cases are positively matched to the reference templates for a False Match Rate (FMR) of 0.1%. As originally suggested by Hill [2001], starting from those synthetic images, Galbally *et al.* [2010a] additionally generate gummy fingers on a Printed Circuit Board. All of them are falsely accepted

as genuine subjects by the verification system for a FMR $< 0.1\%$, thus proving the high quality of the synthetic physical artefacts.

A different approach is followed in [Ross *et al.*, 2007] to reconstruct fingerprint images, in which no iterative technique is considered. Assuming that only the minutiae positions and orientations are available, the orientation field is estimated using minutiae triples. Then, based on the estimated field and the minutiae distribution, the fingerprint class is estimated. Finally, the ridge pattern is synthesised using Linear Integral Convolution. In addition, a rendering step is also undertaken to generate more realistic fingerprints, applying a low-pass filter and histogram equalization.

A second set of reverse engineering methods assumes **knowledge of similarity scores** between probe synthetic images and the enrolled identity, while no knowledge about the structure of the template is assumed. The method proposed in [Adler, 2003] for the reconstruction of face images from Eigenface based templates relies on a hill-climbing optimization of synthetic face images. The authors use the similarity score between the synthetic images and the stored template as feedback to improve the synthetic reconstruction. A more efficient hill-climbing technique is proposed in [Adler, 2004], where each quadrant of the synthetic face image is independently optimized even if only quantized scores are shared by the verification system (as recommended by the BioAPI Consortium [2001]). Analogously, using a Bayesian hill-climbing algorithm, face images are recovered from Eigenface- and GMM parts-based systems in [Galbally *et al.*, 2010b], achieving an acceptance rate of over 85%.

Mohanty *et al.* [2007] reconstruct face images assuming access to the similarity scores between a pool of real face images and the face to be reconstructed. Furthermore, **knowledge of the distance function** used by the particular face verification system is required. In this approach, the authors model the face sub-space with an affine transformation, which is a combination of a PCA baseline and a system dependent non-rigid transformation (i.e., the deviations of each subject from the average face represented by the PCA matrix). In order to reconstruct a particular face enrolled in the system, the distances from the pool of real images to the attacked face are used to compute the point in the affine subspace that corresponds to the attacked identity. Finally, the affine transformation is inverted to obtain the desired face image. The approach was tested on several verification algorithms, achieving an acceptance rate of 73% for a commercial system.

Finally, Venugopalan and Savvides [2011] reconstruct iris images from the iriscodes in a two-step approach, assuming **knowledge of the feature extraction algorithm**. First, using a reversed version of the Gabor function used to extract iriscodes from iris images, and a pool of real iris images, a subject-specific iris pattern is generated. Then, this pattern is embedded into a real iris texture to make the image more realistic.

In the face and iris reconstruction methods mentioned, a set of real images is used to either initialize the optimization process or embed the identity to reconstruct into the subspace. Due to the free access to different face and iris images databases, this is not a strong limitation for the eventual attackers.

It should be finally noted that in the aforementioned studies, and throughout this Dissertation, inverse biometric approaches are analysed from a computer-based perspective: their main goal is the deception of biometric recognition systems, not the visual resemblance with their real counterparts. As a consequence, in those studies the quality of the synthetic samples is analysed launching attacks on recognition algorithms.

2.2. Unimodal Biometric Template Protection

Unimodal Biometric Template Protection schemes, or simply Biometric Template Protection (BTP) schemes, can be used to prevent the success of the inverse biometric approaches reviewed in Sect. 2.1, and thereby enhance the privacy provided by biometric systems. As suggested in [Campisi, 2013; Rathgeb and Uhl, 2011; Tuyls *et al.*, 2007], BTP schemes have been traditionally divided into:

- **Cancelable biometrics**, where biometric samples are permanently and irreversibily transformed, and comparison is carried out in the protected domain.
- **Cryptobiometrics**, where a digital key is either bound or generated from a biometric template.

However, in the last few years, new schemes based on Homomorphic Encryption (HE) and Garbled Circuits (GC) have been proposed, which do not belong to these categories. On the one hand, contrary to cancelable biometric approaches, no information is lost or modified in the protected (or encrypted) domain with respect to the unprotected templates. On the other hand, regarding biometric cryptosystems, a regular cryptographic key is used to encrypt the unprotected templates, instead of bounding or generating it from biometric data, and no decryption of the protected templates is necessary at verification time. As a consequence, in analogy to the wider concept of *privacy-preserving signal processing in the encrypted domain* [Lagendijk *et al.*, 2013], a third class can be added, namely:

- **Biometrics in the encrypted domain**, where techniques such as HE and GC are used to encrypt the reference templates and comparison is carried out in the encrypted domain.

A diagram with the BTP classification followed in this section is shown in Fig. 2.2, where the categories of the novel methods proposed in this Dissertation are highlighted in blue. In addition, Table 2.2 summarises the major advantages and disadvantages of each approach, with respect to the requirements established in Chapter 1, namely: verification accuracy preservation, irreversibility, unlinkability and computational complexity.

In the next sections (Sect. 2.2.2 to Sect. 2.2.4), a summary of the most representative works related to cancelable biometrics, cryptobiometrics and biometrics in the encrypted domain for *unimodal* systems is given.

It is important to note, that a fair comparison between the described schemes is hard to establish. Each system was evaluated on different, and mostly small, databases, under different

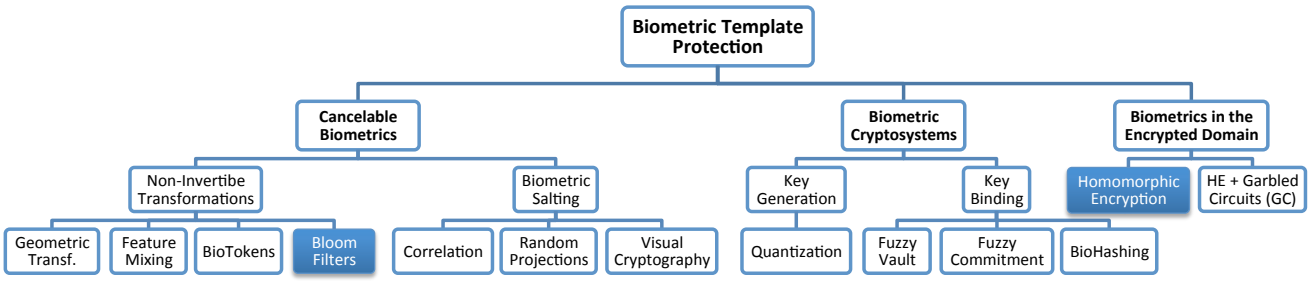


Figure 2.2: *Biometric Template Protection schemes classification. The categories to which the methods proposed in the Dissertation belong are highlighted in blue.*

scenarios. Moreover, approaches show different requirements, such as multi-sample enrolment or mandatory pre-alignment of biometrics samples. Finally, in most cases, even if no attacks have yet been proposed, no thorough irreversibility and/or unlinkability analysis has been performed. In spite of such limitations, in each subsection Tables 2.3 to 2.5 include a summary of the most relevant BTP works in that specific category.

2.2.1. Security and Cryptography Related Terms

Let us introduce some terms, closely related to the fields of security evaluation of biometric systems and cryptography, that will be used in the following:

- *Stolen-token scenario*: evaluation setting in which the impostor is in possession of the genuine token or template, in opposition to the *non-stolen-token scenario*.

- *Public key encryption*: cryptographic algorithms which are based on mathematical problems that currently admit no efficient solution. This techniques use asymmetric key algorithms, where a key used by one party to perform encryption is not the same as the key used by another for decryption. Therefore, each subject has a pair of cryptographic keys - a public encryption key (*public key*, *pk*) and a private decryption key (*secret key*, *sk*). The strength lies in the"impossibility"(computational impracticality) for a properly generated private key to be determined from its corresponding public key. Thus the public key may be published without compromising security, since security depends only on keeping the secret key private.

- *Hash*: a hash function is any function that can be used to map data of arbitrary size to data of fixed size. In particular, a cryptographic hash function is considered practically impossible to invert, that is, to recreate the input data from its hash value alone.

Three different adversary models can be considered:

- *Honest-but-curious model*: both parties, client and server, follow the established protocols but may try to learn additional information about the sample/template on the other side.

Table 2.2: *Summary of advantages and disadvantages of BTP approaches*

	Cancelable Biometrics	**Cryptobiometrics**	**Biometrics in the** Encrypted Domain
Accuracy	Drops	Drops	Preserved
Irreversibility	Permanent protection	Decryption at verification	Permanent protection
Unlinkability	Not analysed	Not analysed	Granted
Computational complexity	Preserved	Preserved	Increased

- *Advanced model*: the adversary has the full knowledge of the algorithms used for template extraction, template protection and comparison, following Kerckhoffs' principles [Kerckhoffs, 1883]. In addition, the adversary is capable of executing part of or all sub-modules of the system that make use of the secret keys, following or not the established protocol, while the adversary knows none of the secrets.
- *Full Disclosure Model*: this model is the advanced model augmented by disclosing the secret keys to the adversary.

2.2.2. Cancelable Biometrics

Cancelable biometrics consist of intentional, repeatable distortions of biometric signals based on transformations which provide a comparison of biometric templates in the protected domain [Ratha *et al.*, 2001]. As shown in Fig. 2.2, there are two main types of cancelable biometric schemes:

- **Non-reversible transformations** of the biometric data or unprotected templates.
- **Biometric salting**, in which Auxiliary Data (AD) is blended with biometric data to derive a distorted version of the biometric template.

One of the earliest methods for generating cancelable biometric templates was based on **non-invertible transforms**. Ratha *et al.* [2001] applied *geometric transformations* in the image domain. At enrolment, the transform (e.g. surface folding) is applied to a facial image using application-dependent parameters. During verification, probe images are transformed employing the same parameters and compared to the stored reference. Several types of transformations, such as block permutation, are proposed in [Ratha *et al.*, 2006, 2007] for fingerprints.

In contrast to those techniques, approaches based on *feature mixing* have been proposed. Jeong *et al.* [2006] combine two different feature extraction methods to achieve cancelable face biometrics: Principal Component Analysis (PCA) and Independent Component Analysis (ICA) coefficients are extracted and both feature vectors are randomly scrambled and added in order to create a transformed template. Regarding variable-length templates, Maiorana *et al.* [2010]

Table 2.3: *Summary of key cancelable biometric schemes. This table is an updated version of Table 8 in [Rathgeb and Uhl, 2011].*

Technique	Characteristic	Reference	Accuracy (%)	Database
Fingerprint	*Non-invertible*: Block permutation	Ratha *et al.* [2007]	FNMR: ~ 35, ~ 15	188 subjects
	Non-invertible: Radial transform Revocable BioTokens	Boult *et al.* [2007]	$\sim 0.08\%$ EER	FVC 2004 (200 subjects)
On-line Signature	*Non-invertible*: BioConvolving	Maiorana *et al.* [2010]	10.81% EER	MCYT (330 subjects)
Face	*Salting*: BioHashing	Teoh *et al.* [2006]	0.0002% EER	ORL-DB/Faces94 (194 subjects)
	Salting: Visual Crypto.	Ross and Othman [2011]	6% EER	XM2VTS (295 subjects)
Iris	*Salting*: Rand. Projection	Pillai *et al.* [2011]	$\sim 2\%$ EER	ND-IRIS-0405 (356 subjects)
	Non-invertible: Bloom Filters	Rathgeb *et al.* [2013b]	1.75% EER	CASIA-v3-Interval (249 subjects)

transform sequences extracted from biometric samples in a two-step approach: each sequence is randomly divided into a fixed number of segments, and those segments are subsequently convolved. These transformed signals are then used for identity verification. A case study is presented for on-line signature, even if the method can be potentially applied to any sequence-based biometric system.

Then, in [Boult, 2006], cryptographically secure *BioTokens* are proposed and applied to existing face recognition schemes, such as PCA. The key idea is to split biometric features into a stable part and an unstable part. For face, the authors suggest to simply split real feature values into an integer part and a fractional part. Subsequently, stable parts are encrypted and unstable parts are obscured applying non-invertible projections. A more thorough analysis of the BioToken concept is carried out in [Boult *et al.*, 2007] for fingerprints, and an improved version is proposed providing increased security, privacy and verification accuracy.

Since all the aforementioned schemes rely on some transformation of the images or derived templates, some accuracy degradation is observed. In opposition to those techniques, one of the last approaches based on non-invertible transformations relies on the extraction of *Bloom filters* [Bloom, 1970] from binary templates, showing no accuracy degradation and achieving rotation-invariant and compressed templates. These filters are essentially a space-efficient probabilistic data structure representing sets to support membership queries, and have been widely used in networking applications [Broder and Mitzenmacher, 2005]. In [Rathgeb *et al.*, 2013a,b], this concept is applied to iriscodes. Similar approaches have been later proposed for fingerprint

templates based on minutiae vicinities [Li *et al.*, 2015] or the Minutiae Relation Code representation [Abe *et al.*, 2015]. In spite of the advantages with respect to other cancelable biometric approaches, Bringer *et al.* [2015] proposed a reconstruction approach for iriscodes given their corresponding Bloom filter templates, able to produce iriscodes which, even if not visually realistic, were positively verified by the original unprotected iris system. Furthermore, some concerns have been raised regarding the unlinkability of the proposed schemes [Hermans *et al.*, 2014].

A second set of cancelable biometric approaches is based on **biometric salting** (see Fig. 2.2), which consists on mixing random or synthetic patterns within biometric templates. The most popular salting technique is the *BioHashing* approach [Goh and Ngo, 2003; Teoh *et al.*, 2006, 2004], initially proposed for face biometrics. Basically, this technique operates as a *key-binding* scheme (see Sect. 2.2.3), using secret subject-specific tokens (private instead of public AD) at verification. Prior to the key-binding step, secret tokens are blended with biometric data to derive a distorted biometric template, hence representing an instance of biometric salting [Rathgeb and Uhl, 2011].

On the other hand, motivated by the success of the *correlation* filter-based methods in pattern recognition and computer vision applications [Patel *et al.*, 2015], Savvides *et al.* [2004] generate cancelable face biometrics applying minimum average correlation filters, where subject-specific secret PINs (secret AD) serve as seed for a random basis of filters.

Another biometric salting approach widely used is based on *random projections*. In [Pillai *et al.*, 2010, 2011] the extracted iriscodes are projected onto a random subspace. Since linear transformations, even if they are independently applied to small sectors of the image, will mix occluded parts of the iris image or reflections with high quality segments of the iris texture, verification accuracy is degraded. Only using a subject-specific random matrix as AD can accuracy be maintained. Similarly, in [Kim and Toh, 2007] subject-specific random projections (AD) are applied to PCA-based face features followed by an error minimizing template transform.

More recently, *visual cryptography* has been proposed for protecting biometric templates. The main idea behind this type of approach is to generate two (or more) random-looking shares from an individual biometric sample, revealing no biometric information, and store them in separate databases. Only using all shares can we recover the original biometric image. In that context, Ross and Othman [2011] present two different schemes for face, and for iris or fingerprints. The main difference between both methods is that, for face biometrics, a public image (AD) is combined with the face sample to generate two different shares. Even if almost no accuracy degradation is observed in these methods for the non-stolen-token scenario, they present two main drawbacks: on the one hand, two (or more) databases need to be handled, hence increasing the complexity of the system. On the other hand, should the databases be compromised, the original biometric sample or template can be recovered, thereby compromising the privacy of the subject.

It should be noted that in most biometric salting approaches [Savvides *et al.*, 2004; Teoh *et al.*, 2004], subject-specific keys (secret AD) are incorporated while experiments are performed under the non-stolen-token scenario, hence omitting the actual biometric accuracy of the system

[Kong *et al.*, 2006; Rathgeb and Uhl, 2010c]. For instance, in follow-up publications [Teoh and Ngo, 2006; Teoh *et al.*, 2008], a significant degradation of verification accuracy is reported for the stolen-token scenario.

Finally, in the vast majority of approaches to cancelable biometrics, revocability is provided by incorporating secret credentials, e.g. random numbers. That is, in order to generate the protected template $\mathbf{C}$, the *PIE* may take as input a secret key $\mathbf{K}$, as well as the biometric data, $\mathbf{B}$: $\mathbf{C} = \mathrm{PIC}(\mathbf{B}, \mathbf{K})$. The key $\mathbf{K}$ is system dependent and different protected templates might be generated from the same biometric sample using different keys: $\mathbf{C}_i = \mathrm{PIC}(\mathbf{B}, \mathbf{K}_i)$. Even thought the key should be kept secret, in an ideal scenario, knowledge of this key by an eventual attacker would not disclose any information about the unprotected template $\mathbf{T}$ or the original biometric sample $\mathbf{B}$. Consequently, not only accuracy but also irreversibility or unlinkability evaluations have to be performed under the "stolen-token scenario", where an impostor is in possession of valid secrets.

2.2.3. Cryptobiometric Systems

These methods combine cryptographic keys with transformed versions of the original biometric templates to obtain secure templates. In most cases, some public information, known as *helper data* or *auxiliary data*, is generated. As depicted in Fig. 2.2, depending on how the AD is used, cryptobiometric schemes can be broadly divided into:

- **Key binding** schemes, where AD are obtained combining the key with the biometric template. At verification time, applying an appropriate key retrieval algorithm to the probe biometric sample, the key is obtained from the AD.

- **Key generation** schemes, where both the AD and the key are generated directly from biometric data. Again, at verification time, a key is recovered from the probe sample using the AD.

Most cryptobiometric systems rely on the fuzzy vault [Juels and Sudan, 2006] and the fuzzy commitment [Juels and Wattenberg, 1999] schemes, which are classified as **key binding** approaches.

In *fuzzy commitment* schemes, a witness (biometric data) is committed to a codeword (error correcting code, EEC). The difference between them and a hash value of the codeword are stored as AD. At verification time, the difference vector is used to reconstruct the codeword from the acquired biometric sample, and its corresponding hash is compared to the one stored as part of the AD.

Hao *et al.* [2006] apply this paradigm to iriscodes, using Hadamard and Reed-Solomon EEC. Bringer *et al.* [2007] later proposed a two-dimensional iterative min-sum decoding with Reed-Muller codes to obtain a more efficient decoding. Several improvements for such systems have been proposed in successive works [Ignatenko and Willems, 2009a; Rathgeb and Uhl, 2010a].

Table 2.4: *Summary of key biometric cryptosystems. This table is an updated version of Table 7 in [Rathgeb and Uhl, 2011].*

Technique	Characteristic	Reference	FNMR/FMR	Database
Key Binding: Fuzzy commitment	Iris	Hao *et al.* [2006]	0.42 / 0.0	70 subjects
		Bringer *et al.* [2007]	5.62/0.0	ICE 2005 (244 subjects)
	Fingerprint	Nandakumar [2010]	12.6/0.0	FVC2002-DB2 (110 subjects)
	Signature	Argones-Rua *et al.* [2012]	2.93/2.64	MCYT (100 subjects)
Key Binding: Fuzzy vault	Fingerprint	Nandakumar *et al.* [2007]	4.0 / 0.004	FVC2002-DB2 (110 subjects)
	Iris	Wu *et al.* [2008a]	5.5 / 0.0	CASIA v1 (108 subjects)
	Palmprint	Wu *et al.* [2008b]	0.73 / 0.0	PolyU DB (750 subjects)
Key Binding: BioHashing	Face	Teoh *et al.* [2004]	0.0 / 0.0	ORL-DB/Faces94 (194 subjects)
Key Generation: Quantization	On-line Signature	Feng and Wah [2002]	28.0 / 1.2	750 subjects
		Vielhauer *et al.* [2002]	7.05 / 0.0	10 subjects

Although the fuzzy commitment paradigm was first applied to iris biometrics, it has been also applied to other binary templates. For instance, Teoh and Kim [2007] binarized fingerprint features applying a randomized dynamic quantization transformation, and subsequently used Reed-Solomon codes to construct the fuzzy commitment scheme. The transformation consists on a subject-specific non-invertible projection, hence requiring the secure storage of a subject token. Similar approaches have been also applied to face hashes in [Zeng and Watters, 2007]. Also for face biometrics, Lu *et al.* [2009] propose a fuzzy commitment scheme for binarized PCA based features. More recently, Nandakumar [2010] presented a fuzzy commitment scheme for a binary fixed-length representation of fingerprints, based on a quantization of the Fourier spectrum of minutiae sets. Alignment was achieved using high curvature regions.

Regarding behavioural biometrics, subject adaptive EECs were applied in [Maiorana *et al.*, 2008] to on-line signature, where the error correction information is selected for each subject based on the intra-variability of the particular subject's data. More recently, the fuzzy commitment paradigm was applied in [Argones-Rua *et al.*, 2012] to an on-line signature verification system based on a combination of Universal Background Models (UBM) with Hidden Markov Models (HMM), achieving a remarkable verification accuracy.

On the other hand, the key idea of the *fuzzy vault* scheme is to use an unordered set to lock a secret key. The resulting vault can be unlocked with another set similar enough to the

original one, thus allowing the reconstruction of the key, and thereby verifying the identity of the subject. The vault is created applying polynomial encoding and error correction.

The first practical implementation of the fuzzy vault scheme in biometrics was proposed by Clancy *et al.* [2003] for minutiae-based fingerprint templates. Fingerprints were assumed to be pre-aligned. Later on, Nandakumar *et al.* [2007] suggested the use of high curvature points of the fingerprint orientation field as AD to solve the pre-alignment issues. Similarly, in [Levi *et al.*, 2006] a biometric cryptosystem based on minutiae extracted from on-line signatures and the fuzzy vault paradigm was presented.

On the other hand, Wu *et al.* [2008a] proposed a fuzzy vault based on iris, where the iris texture is divided into 64 blocks and the mean gray scale value is computed. In a subsequent work, Wu *et al.* [2008b] presented a system based on the features extracted with Gaussian derivative filters from palmprint samples.

Finally, the *BioHashing* [Teoh *et al.*, 2004] approach described in the previous section can be also classified as a key-biding cryptobiometric system.

In spite of the advantages of these key-binding schemes, such as compact representation or easy key update, several works have proven that fuzzy schemes are vulnerable to attacks on the AD that compromise the security of the system and the privacy of the subjects [Ignatenko and Willems, 2009b, 2010; Rathgeb and Uhl, 2012; Scheirer and Boult, 2007].

Regarding **key generation** cryptobiometric systems (see Fig. 2.2), *quantization* schemes model the enrolment samples with intervals for each real-valued feature. Such intervals are encoded as integer values and stored as AD. At verification time, the characteristics of the newly presented sample are extracted and mapped into the previously defined intervals, generating a hash or key. Feng and Wah [2002] proposed an scheme for on-line signature, aligning the samples with a Dynamic Time Warping algorithm. Similarly, Vielhauer *et al.* [2002] generated hashes using interval matrices for each subject. More recently, Freire *et al.* [2007] proposed a biometric cryptosystem based on hashes generated from templates comprising signature global features. On the other hand, a BCH error correcting code and AD are used in the template protection scheme presented in [Freire *et al.*, 2008].

Although quantization schemes have been extensively applied to signature data, they have been also applied to other biometric characteristics. For instance, Sutcu *et al.* [2005] present a general method for extracting hashes from biometric data, applying it to face samples. This approach was extended to iris biometrics by Rathgeb and Uhl [2009], obtaining longer hashes.

Again, the main drawbacks of such quantization based techniques are the accuracy degradation due to the loss in accuracy of converting the original real-valued features to integer-valued intervals, and potential attacks on the stored AD. Since such data comprise subject-specific intervals for each feature, a potential attacker could easily reconstruct a template to impersonate a genuine subject.

Table 2.5: *Summary of key biometrics in the encypted domain schemes.*

Technique	Characteristic	Reference	Accuracy	Database
HE	Fingerprint	Barni *et al.* [2010]	$\sim$ 7% EER	Crossmatch 52 subjects
	Face	Erkin *et al.* [2009]	96% Det. Rate	ORL Face (40 subjects)
HE + GC	Iris	Blanton and Gasti [2011]	Not reported	

2.2.4. Biometrics in the Encrypted Domain

As an alternative to the aforementioned methods based on cancelable biometrics or cryptobiometrics, Homomorphic Encryption schemes allow for computations to be performed on ciphertexts, with no additional AD, and which generate encrypted results which decrypt to plaintexts that match the result of the operations carried out on the original plaintext [Fontaine and Galand, 2007]. Therefore, combining such an encryption approach with biometric verification systems would meet the irreversibility and unlinkability requirements while preserving verification accuracy [Barni *et al.*, 2015]. Since practical implementations of Fully Homomorphic Encryption (FHE) schemes still remain a big challenge [Aguilar-Melchor *et al.*, 2013], semi Homomorphic Encryption (HE) schemes, which only allow a limited subset of operations in the encrypted domain, are nowadays being introduced into many applications based on signal processing [SPM, 2013; Aguilar-Melchor *et al.*, 2013; Troncoso-Pastoriza and Perez-Gonzalez, 2013], and, particularly, biometrics [Barni *et al.*, 2010; Bringer *et al.*, 2013; Ye *et al.*, 2009]. In particular, current approaches to biometric verification in the encrypted domain [Bringer *et al.*, 2013] are based on *Garbled Circuits* (GC) [Yao, 1986] and *Homomorphic Encryption* (HE) [Aguilar-Melchor *et al.*, 2013; Fontaine and Galand, 2007], as shown in Fig. 2.2.

Since efficient implementations of HE schemes are very recent [Paillier, 1999], only a few *unimodal* biometric systems based on this protection technology have been proposed so far. In [Barni *et al.*, 2010], the authors present a new fingerprint verification system based on the FingerCode fixed-length representation of fingerprints [Jain *et al.*, 1999] and HE. Results show that verification accuracy is preserved. However, the database stored in the server is not encrypted and results are reported on a small database comprising data belonging to only 51 subjects. An improved version of that approach is suggested in [Bianchi *et al.*, 2010], where a more compact implementation using quantization is proposed at a small cost in terms of verification accuracy.

In [Erkin *et al.*, 2009], Eigenface based templates are protected with HE. Then, a more efficient approach is presented in [Sadeghi *et al.*, 2010] using GCs for the threshold comparison. Furthermore, the SCiFI project [Osadchy *et al.*, 2010] proposes a biometric identification algorithm specifically designed for a more efficient usage in secure computation, based on fixed-length templates with a constant Hamming weight. In contrast to the Eigenface based approaches, only the matching process, but not the template construction, is secured.

In [Blanton and Gasti, 2011], a secure iris BTP based on a combination of HE and GCs is proposed, handling encrypted iriscodes. In order to deal with the computation of Hamming Distances in the encrypted domain (divisions are not supported), the division and comparison with a verification threshold is reduced to a inequality comparison carried out with GCs. Even though the use of GCs increases the number of computations we can carry out in the encrypted domain, complexity is increased due to the fact that they have to be designed and evaluated ad-hoc.

More recently, Bringer *et al.* [2014a] propose an efficient implementation, known as GSHADE, of several metrics, including the scalar product, the Hamming, Euclidean and Mahalanobis distances. Using oblivious transfers, both the computation time and the bandwidth requirements are improved by a least one order of magnitude with respect to the algorithms proposed in previous works [Blanton and Gasti, 2011; Osadchy *et al.*, 2010].

Finally, a different approach, in which all computations are carried out on the server side, with no interaction with the client, is proposed in [Troncoso-Pastoriza *et al.*, 2013]. Using ideal lattices and a Support Vector Machine (SVM) over Gabor-based face templates, high verification accuracy rates are obtained on three widely used databases, at the cost of higher communication requirements than those of interactive schemes.

It should be noted that alignment issues in the encrypted domain are not always considered [Erkin *et al.*, 2009; Osadchy *et al.*, 2010; Sadeghi *et al.*, 2010]. On the other hand, for iriscodes [Blanton and Gasti, 2011] and fingerprints [Barni *et al.*, 2010] the authors suggest applying matching operations on different rotations on the inputs, as in most unprotected verification schemes, thus leading to a higher computational load.

2.3. Multi-Biometric Template Protection

While all the techniques mentioned in Sect. 2.2 are theoretically sound, they seldom guarantee the desired irreversibility and unlinkability properties without significantly degrading the recognition accuracy [Nandakumar and Jain, 2015]. This limitation can be overcome by introducing *multi-biometric* template protection schemes (MBTP) [Nagar *et al.*, 2012], since the combination of different biometric characteristics generally leads to higher accuracy [Ross *et al.*, 2006]. As defined in the ISO/IEC TR 24722 on multimodal and other multi-biometric fusion [ISO/IEC JTC1 SC37 Biometrics, 2007], fusion can be carried out at three different levels [Ross *et al.*, 2006], namely:

- *Feature level fusion*: a single template of higher dimensionality is generated from the individual templates extracted from each characteristic, hence comprising more discriminative information than each single template.

- *Score level fusion*: each unimodal system returns an individual similarity score, which are normalized to a common range and combined in order to obtain a more accurate system [Poh and Kittler, 2012].

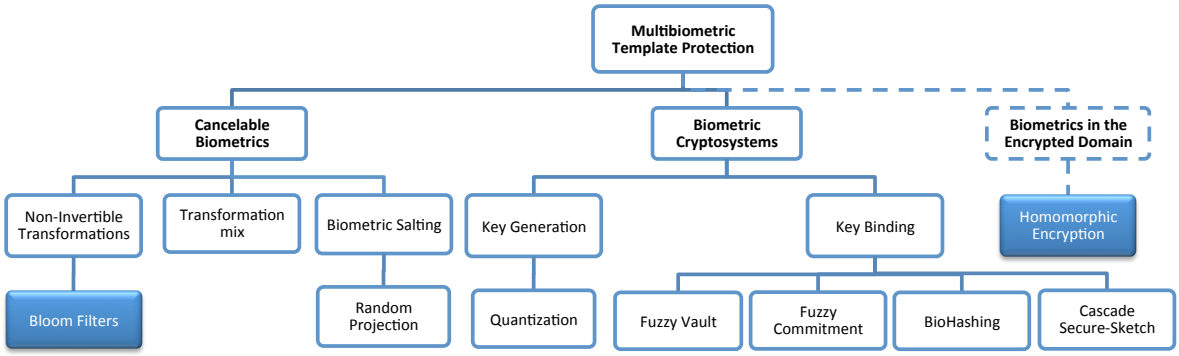


Figure 2.3: *Multibiometric Biometric Template Protection schemes classification. Dashed lines refer to categories for which no multi-biometric template protection schemes have been proposed yet. The categories to which the methods proposed in the Dissertation belong are highlighted in blue.*

- *Decision level fusion*: each unimodal system returns an individual accept/reject decision, which are fused in order to increase the accuracy of the system.

Even though extensive research has been carried out on the fields of multi-biometric recognition [Ross *et al.*, 2006] and *unimodal* biometric template protection [Rathgeb and Uhl, 2011], several issues remain unsolved in the development of *Multi-Biometric* Template Protection (MBTP) schemes [Rathgeb and Busch, 2012]. Two of the most significant challenges are: *i*) the development of a generic framework for multi-biometric template protection, and *ii*) the difficulty to obtain protected templates from non pre-aligned samples, without requiring AD (and hence avoiding potential information leakage).

Fig. 2.3 shows the classification of the MBTP methods followed during the Dissertation, where the categories of the novel methods proposed in this Dissertation are highlighted in blue. As it may be observed, a very reduced subset of cancelable biometric approaches is depicted with respect to the unimodal BTP classification (see Fig. 2.2) and the biometrics in the encrypted domain class is shown in dashed lines: so far, no MBTP schemes have been proposed, which fall into those categories.

In the next subsections, the approaches proposed so far for MBTP systems are described, and summarised in Table 2.6. As it may be observed, the first five rows comprise schemes designed for the fusion of several instances of the same biometric characteristic. It should be also noted that an evaluation of the corresponding biometric systems using unprotected data is presented in very few cases, thereby preventing the assessment of the accuracy degradation due to the protection mechanism.

2.3.1. Cancelable Multi-Biometrics

As shown in Fig. 2.3, MBTP have only been proposed for a very reduced subset of **non-invertible transformations** and **biometric salting** approaches. Rathgeb and Busch [2014] propose the fusion of both iris samples belonging to a given subject using Bloom filters. Paul and Gavrilova [2012] present a fusion of face and ear samples using *random projections* and a

transformation-based feature extraction, reducing dimensionality with PCA and clustering the features with k-Nearest Neighbours (k-NN) classifiers.

Since in multi-biometric systems several samples are used for verifiaction, different transformations can be applied to each of them to enhance the security and accuracy of biometric systems. Since the transformations chosen can be either non-invertible or biometric salting, they are a new subset of cancelable biometrics approaches referred to as **transformation mix** in Fig. 2.3. In that context, Canuto *et al.* [2013] propose the application of BioHashing, interpolation and convolution to voice and iris data. The effects of each transformation on each individual characteristic are analysed, and then fusions of templates generated with the same or different transformations, using ensemble systems with Support Vector Machines (SVM) or k-NN training methods, are compared. As a result of this analysis, the authors proved that the use of different cancelable transformations is more efficient.

In an analogous manner, Othman and Ross [2013] fuse the spiral and the continuous components belonging to two different fingerprints from the same subject into one cancelable template. While the authors showed that the mixed fingerprint representing a new identity can potentially be used for verification, being the mixed fingerprint dissimilar from the original ones and robust to cross-matching attacks, further work is required to enhance the verification accuracy.

2.3.2. Multi-Biometric Cryptosystems

As in the *unimodal* schemes, most multi-biometric cryptosystems based on the **key-binding** concept rely on the *fuzzy vault* [Juels and Sudan, 2006] and the *fuzzy commitment* [Juels and Wattenberg, 1999] schemes. A fuzzy vault scheme is proposed in [Nandakumar and Jain, 2008], where a single multi-biometric template is derived from fingerprint and iris features. Similarly, Bringer *et al.* [2014b] propose the feature-level fusion of several fingerprints applying the fuzzy vault scheme to the ORed individual fixed-length binary templates, based on minutiae vicinities. On the other hand, a fuzzy commitment scheme for the fusion of two different feature extraction algorithms is applied to 3D face data in a single sensor scenario in [Kelkboom *et al.*, 2009].

As pointed out in Sect. 2.2.3, the fuzzy vault scheme is vulnerable to attacks correlating different templates of the same subject. Secondly, auxiliary alignment data, stored as AD, may leak information about the protected templates which negatively affects security and privacy. To avoid those problems, Tams *et al.* [2015] use alignment-free fingerprint features and fuse several samples, thereby removing the need to store alignment parameters. Furthermore, the features are passed through a quantization scheme and then dispersed, thereby thwarting correlation attacks.

Additionally, fuzzy schemes can be applied to secure sketches, that is, secure representations of biometric templates in which AD is used to recover the original biometric template and matching is reduced to an error correction [Verbitskiy *et al.*, 2010]. In [Nagar *et al.*, 2012], a single secure sketch is generated from multiple and heterogeneous templates, based on the concatenation of the individual sketches. Practical implementations for fuzzy vault and fuzzy commitment schemes are then proposed for the fusion of iris, fingerprint and face.

Table 2.6: *Summary of key multi-biometric template protection schemes.*

Characteristic	Technique	Reference	Accuracy	Database
Fingerprints	*Cancelable*: Mixing Fingers	Othman and Ross [2013]	6% EER	WVU (500 subjects)
	Cryptobiometrics: Fuzzy vault	Bringer *et al.* [2014b]	0.27 / 0.009	FVC2002-DB2 (110 subjects)
		Tams *et al.* [2015]	82% GAR 0% FMR	FVC2002-DB1 (110 subjects)
Face	*Cryptobiometrics*: Fuzzy commitment	Kelkboom *et al.* [2009]	2.45% EER	FRGC v2 (454 subjects)
Iris	*Cancelable*: Bloom Filters	Rathgeb and Busch [2014]	0.48 EER	IITD v1 (224 subjects)
Iris + Face + Fingerprint	*Cryptobiometrics*: Fuzzy Vault & Commit.	Nagar *et al.* [2012]	68% GAR 75% GAR	WVU (138 subjects)
Face + Ear	*Cancelable*: Random projection	Paul and Gavrilova [2012]	89% GAR 0% FMR	AT&T + UPM (17 subjects)
Voice + Iris	*Cancelable*: BioHashing, Interp. BioConvolving	Canuto *et al.* [2013]	$\sim$ 95% GAR	TIMIT + CASIA v1 (100 subjects)
Iris + Fingerprint	*Cryptobiometrics*: Fuzzy vault	Nandakumar and Jain [2008]	1.8 / 0.01	CASIA + MSU-DBI (108 subjects)
	Cryptobiometrics: Cascade	Cimato *et al.* [2008]	0% EER	CASIA + FVC2000 (108 subjects)
Face + Fingerprint	*Cryptobiometrics*: Quantization	Sutcu *et al.* [2007]	0.92 / 0.0002	Faces94 + NIST (152 subjects)

In opposition to those previous schemes, a modular approach for the design of multi-biometric cryptosystems is proposed in [Cimato *et al.*, 2008]: a secure sketch is extracted from each biometric template, and used in a sequential manner to secure successive templates. In [Fang *et al.*, 2010], a more general approach is presented, where multiple secrets are similarly used in a cascade fashion within the secure sketch framework. In this last case, no evaluation of the verification accuracy is provided. These approaches, classified as *key binding* schemes, have the advantage of an easy escalation to more biometric samples, while the main limitation is that the overall security is bounded by the security of the outermost layer.

On the other hand, regarding *key generation* systems, quantization schemes are applied to SVD-based face features and pre-aligned minutiae-based fingerprint templates in [Sutcu *et al.*, 2007] to generate a single secure sketch. Even though a good accuracy is achieved with a simple and efficient fusion, and the security of the template is analysed, the authors point out that one

of the open issues is how to determine the exact information leakage due to the sketch.

2.4. Chapter Summary and Conclusions

In this chapter we have summarised the main works related to this PhD Thesis. We have started by describing the main threats to biometric recognition systems in terms of privacy vulnerabilities: inverse biometric algorithms. A taxonomy of those methods has been presented and the most important works in each category summarised. Then we have focused on Biometric and Multi-Biometric Template Protection schemes as a countermeasure to minimize the potential privacy leakage derived from the storage of unprotected biometric templates. The main works proposed have been presented and categorized.

Being this chapter a summary of the state-of-the-art, no new material has been presented. Although the exposition of certain parts of the chapter is based on some of the cited publications, most of the structure and presentation has followed a personal perspective.

Chapter 3

Security and Privacy Evaluation of Biometric Systems

This chapter summarizes the common practices in accuracy testing of biometric systems and presents the evaluation methodology followed in the Thesis for the security and privacy assessment of unprotected and protected biometric systems.

In order to meet the right of privacy preservation of the subjects, biometric templates need to be protected and biometric systems should be thoroughly evaluated, taking into account the privacy issues exposed in Chapter 1, Sect. 1.2. While certain properties are inherent to the templates (e.g., irreversibility, unlinkability), other performance measurements (e.g., accuracy) can only be analysed at system level. To assess those requirements, in this chapter we propose: *i*) a general framework for the evaluation of unprotected and protected biometric systems, and *ii*) a new framework for the unlinkability assessment of protected biometric templates.

The chapter is organized as follows. First we summarize the guidelines for accuracy analysis of biometric systems (Sect. 3.1). Then we provide a description of the proposed protocol for the privacy and security evaluation of unprotected and protected biometric schemes followed in the Thesis (Sect. 3.2). Finally we give an overview of the baseline unprotected systems (Sect. 3.3) and biometric databases (Sect. 3.4) used in the Dissertation.

This chapter is based on the publications: Galbally *et al.* [2013]; Gomez-Barrero *et al.* [2014b, 2016d].

3.1. Accuracy Analysis of Biometric Systems

As it will be later described in Sect. 3.2, in order to assess the security and privacy provided by traditional (or unprotected) biometric systems and biometric template protection (BTP) schemes, we first need to analyse the accuracy of such systems. To that end, the first research works on biometrics [Atal, 1976; Kanade, 1973; Nagel and Rosenfeld, 1977] reported experimental results using biometric data specifically acquired for the experiment at hand. In contrast to such

practice, a fair comparison of different recognition strategies can be established using common and publicly available benchmarks [Jain *et al.*, 2011; Phillips *et al.*, 2000a]. In this context, the UK Biometrics Working Group has generated a set of best practices for testing and reporting accuracy results of biometrics systems [Mansfield and Wayman, 2002], to which we adhere in this PhD Thesis.

Among the three different levels defined by Phillips *et al.* [2000b] for accuracy analyses (i.e., technology, scenario and operational), in this Thesis we focus on technology evaluations of different systems working in the *verification* mode. The goal of a technology evaluation is to compare several algorithms, thereby identifying the most promising recognition approaches and tracking the state-of-the-art. Testing of all algorithms is carried out on a standardized database, so that the tests are repeatable.

As described in Chapter 1, under the verification mode, the subject issues a positive claim of identity (i.e., I am John Doe), and the system carries out a one-to-one comparison of the submitted sample to the enrolled template for the claimed identity. Mansfield and Wayman [2002] define two types of access attempts in the normal operation scenario of a verification biometric system: *i*) *biometric mated comparison trial*, where a subject makes a truthful positive claim about his own identity in the system (the probe sample matches the reference template), and *ii*) *biometric non-mated comparison trial*, where a user makes a false positive claim about another identity in the system (the probe sample does not match the reference template). Mated trials are also referred to as *client* or *genuine* attempts, while non-mated trials are also known as *impostor* or *zero-effort* attempts, and constitute the most basic form of attack to a biometric system.

Considering these two different types of access attempts, biometric authentication can be considered as a detection task, involving a trade-off between two types of errors [Mansfield and Wayman, 2002]: *i*) False Non-Match (FNM), occurring when a user making a mated claim of identity is rejected by the system, and *ii*) False Match (FM), taking place when a user making an non-mated claim of identity is accepted into the system. In order to estimate the False Non-Match Rate (FNMR) and False Match Rate (FMR) of a given system, a set of mated and non-mated matching scores (resulting respectively from mated and non-mated trials) have to be generated using the available biometric data. Several methods have been described in the literature in order to maximize the use of the information embedded in the training samples during a test including resubstitution, holdout, cross-validation, and variants of the jackknife sampling using the leave-one-out principle [Jain *et al.*, 2000; Theodoridis and Koutroumbas, 2008].

Although each type of error can be computed for a given decision threshold, a single accuracy level is inadequate to represent the full capabilities of the system. Therefore the accuracy capabilities of authentication systems have been traditionally shown in the form of FM and FNM Rates versus the decision threshold. A commonly used graphical representation of the capabilities of an authentication system, specially useful when comparing multiple systems, is the ROC (Receiver -or also Relative- Operating Characteristic) plot, in which FM Rate (FMR)

versus FNM Rate (FNMR) is depicted for variable decision threshold. A variant of the ROC curve, the so-called DET (Detection Error Tradeoff) plot, is used in this Thesis [Martin *et al.*, 1997]. In this case, the use of a non-linear scale makes the comparison of competing systems easier.

A specific point is attained when FMR and FNMR coincide, the so-called EER (Equal Error Rate). The global EER of a system can be easily detected by the intersection between the DET curve of the system and the diagonal line y = x. Nevertheless, and because of the discrete nature of FMR and FNMR plots, EER calculation may be ambiguous according to the above-mentioned definition, so an operational procedure for computing the EER must be followed. In the present contribution, the procedure for computing the EER described by Maio *et al.* [2002b] has been applied. Furthermore, in accordance with ISO/IEC IS 19795-1 [ISO/IEC JTC1 SC37 Biometrics, 2006], FNMR for a specific FMR values are reported.

3.2. Security and Privacy Evaluation of Biometric Systems

As mentioned in Chapter 1, Sect. 1.2, in order to ensure the necessary privacy to the subjects, the following issues regarding biometric systems should be taken into account:

- Do the stored templates reveal any information about the original biometric samples? In other words, are we able to reconstruct synthetic samples whose templates are similar enough to those of the original subject?
- Are my enrolled templates in different recognition systems somehow related to each other? Can someone cross-match those templates and track my activities?
- What if someone steals a template extracted from (for instance) my right index finger? Won't I be able to use that finger again to enrol into the system? Has it been permanently compromised?

In accordance with the ISO/IEC IS 24745 on biometric information protection [ISO/IEC JTC1 SC27 IT Security Techniques, 2011], to cope with these issues, protected and unprotected biometric systems should comply with three main requirements:

- **Irreversibility** of the templates, so that no biometric information can be derived from the stored references.
- **Unlinkability** of the templates, in order to prevent tracking subjects among different applications for which the same biometric characteristic has been used for enrolment. Additionally, in order to tackle with the last issue and provide templates' revocability, different templates should be generated from a single biometric instance of a given subject.
- **Accuracy** of the system should be maintained with respect to the unprotected system, in case a biometric template protection (BTP) algorithm is introduced.

To assess whether those properties are met for a particular biometric system, a security and privacy evaluation is carried out. In order to follow a systematic protocol, thereby ensuring reproducibility and future comparisons with the state-of-the-art, such an evaluation comprises seven steps:

1. Description of the biometric system that will be evaluated (the baseline unprotected biometric systems used in the present Dissertation are described in Sect. 3.3).

2. Description of the database that will be used in the evaluation (the biometric databases used in the present Dissertation are described in Sect. 3.4).

3. Description of the information about the system under evaluation required to be known by the eventual attacker.

4. Description of the experimental protocol that will be followed in the accuracy, irreversibility and unlinkability analyses that will be carried out in the next steps.

5. Execution of an accuracy analysis of the system being tested (see Sect. 3.2.3).

6. Execution of the irreversibility analysis of the templates (see Sect. 3.2.1).

7. Execution of the unlinkability analysis of the templates (see Sect. 3.2.2).

Each particular analysis (steps 5 to 7) is defined in the next sub-sections.

It should be noted that, if templates are reversible, they are also linkable, since unlinkability is a stronger condition on the templates. If we are able to reconstruct the biometric sample from the information stored in the templates, we will then be able to link those reconstructed samples. On the other hand, even if we are not be able to extract enough information to recover the biometric sample protected within the template, we still might be able to decide whether two templates conceal the same identity. As a consequence, if templates fail to pass the irreversibility analysis, there is no need to conduct the unlinkability analysis.

3.2.1. Irreversibility Analysis of Templates

In order to address the first privacy issue, that is, study whether templates reveal any biometric information of the subject, the irreversibility of the templates is studied. The main goal of this analysis is to evaluate the feasibility of reverting the feature extraction process that, in principle, should conceal our biometric data. To that end, inverse biometrics attacks such as the ones proposed in Chapter 4 will be carried out on unprotected biometric templates. As explained in Chapter 2, the aim of these attacks is to reconstruct synthetic biometric samples which are positively matched to the stored reference template by the system.

The analysis of *unprotected templates* will therefore comprise two consecutive steps:

- Reconstruct synthetic samples for a particular instance, using an inverse biometrics method.

- Present those synthetic samples to the system, and evaluate the chances of deceiving it, in terms of the Success Rate (SR) of the attack.

This way, for a given operating point of the system (see Sect. 3.1), the performance of the attack is measured in terms of its Success Rate (SR), which is the expected probability that the attack successfully reconstructs a given sample, thereby achieving the impersonation of a subject. It is computed as the ratio between successful attacks (A_s) and the total number of attacks carried out (A_T):

$$\mathrm{SR} = A_s/A_T \times 100 \tag{3.1}$$

This measure gives an estimation of how dangerous it is a particular attack for a given biometric system: the higher the SR, the bigger the privacy threat. Or, in other words, the more reversible the templates. Since in general the success of an attack is highly dependent on the FMR of the system, the vulnerability of the system to the attacks with the reconstructed images should be evaluated at different operating points. We propose the analysis at the points corresponding to FMR = 0.1%, FMR = 0.05%, and FMR = 0.01%, which, according to [ANSI-NIST, 2001], correspond to a low, medium and high security application, respectively. For completeness, systems should be also tested at very high security operating points, for example those corresponding to FMR $\ll$ 0.01%.

Regarding BTP schemes based on a transformation of the templates (such as those proposed in Chapters 5 and 6), we may assume that such reverse engineering process is eventually possible for any given unprotected template. Therefore, in order to analyse protected templates, we will restrict to reversing the protection technique in order to reconstruct the original unprotected references. In an analogous manner to the aforementioned analysis of unprotected templates, we will try to access the baseline unprotected system with those reconstructed templates, reporting the SR of such attempts or analysing the score distributions of real and reconstructed templates. As a consequence, the steps to be followed in the analysis of *protected templates* are:

- Starting from a *protected* template, try to reconstruct its corresponding *unprotected* template, taking advantage of a known weakness in the protection algorithm.
- Present those reconstructed *unprotected* templates to the system, and analyse the score distributions yielded by real and reconstructed unprotected templates.

3.2.2. Unlinkability Analysis of Templates

In order to provide unlinkability, secret keys are commonly introduced into template protection schemes. The *key space size* $|\mathbf{K}|$ is thus required to be large enough such that brute force attacks on the key space should at least be as hard as a false acceptance attack, i.e. $|\mathbf{T}| \geq FMR^{-1}$ [Cavoukian and Stoianov, 2009], where *FMR* is the False Match Rate of the protected system. As a consequence, in order to utilize the entire space of secret keys, a small distance between two keys should cause a large distance between the resulting protected templates [Argones-Rua *et al.*, 2012; Ferrara *et al.*, 2014].

An additional threat can arise from *linkage* or *cross-matching attacks*, where an eventual attacker is in possession of two protected templates $\mathbf{C}^1 = PIE(\mathbf{B}_1, \mathbf{K}_1)$, and $\mathbf{C}^2 = PIE(\mathbf{B}_2, \mathbf{K}_2)$, with $\mathbf{K}_1 \neq \mathbf{K}_2$. His goal is to determine whether both protected templates, $\mathbf{C}^1$ and $\mathbf{C}^2$, conceal the same biometric datum $\mathbf{B}$ (i.e., $\mathbf{B}_1 = \mathbf{B}_2$?), or different samples of biometric data extracted from a the same biometric instance - e.g., the same right index finger.

To prevent such attacks, the dissimilarity score between those templates is required to be higher than a certain decision threshold τ, used to take a final non-match verification decision: $s = PIC(\mathbf{C}^1, \mathbf{C}^2) > \tau$. Furthermore, given two biometric samples $\mathbf{B}_1$ and $\mathbf{B}_2$ obtained from different biometric instances, and two different keys $\mathbf{K}_1$ and $\mathbf{K}_2$, the following equations to compute the dissimilarity score s should hold:

$$s = PIC(\mathbf{C}_1, \mathbf{C}_2) > \tau \begin{cases} \mathbf{C}^1 = PIE(\mathbf{B}_1, \mathbf{K}_1), \mathbf{C}^2 = PIE(\mathbf{B}_1, \mathbf{K}_2), \\ \mathbf{C}^1 = PIE(\mathbf{B}_1, \mathbf{K}_1), \mathbf{C}^2 = PIE(\mathbf{B}_2, \mathbf{K}_1). \end{cases} \tag{3.2}$$

As we will explain below, in order for Eq. 3.2 to hold, there has to be a specific overlap between the inter-class distributions of non-mated comparisons using different keys and the score distribution obtained by comparing identical biometric instances protected with different keys [Ferrara *et al.*, 2014].

To extend formality to the problem being addressed, some mathematical notations are introduced in this section. Let us define the following hypothesis:

$$H_m = \{\text{both templates belong to mated instances}\} \tag{3.3}$$

$$H_{nm} = \{\text{both templates belong to non-mated instances}\} \tag{3.4}$$

Two types of score distributions will be analysed for the assessment of the unlinkability provided by protected templates:

- *Mated instances*: scores computed from templates extracted from different samples of a single instance of the same subject using different keys. It represents the probabilities $p(s|H_m)$, where s is the dissimilarity score between two templates.
- *Non-mated instances*: scores yielded by templates generated from samples of different instances using different keys. It represents $p(s|H_{nm})$.

In this context, we assume that the attacker:

- Is in possession of two protected templates $\mathbf{C}^1 = PIE(\mathbf{B}_1, \mathbf{K}_1)$, and $\mathbf{C}^2 = PIE(\mathbf{B}_2, \mathbf{K}_2)$, where $\mathbf{K}_1 \neq \mathbf{K}_2$.
- Can access the similarity score between them, $s = PIC(\mathbf{C}^1, \mathbf{C}^2)$.
- Knows the *Mated instances* and *Non-mated instances* distributions.

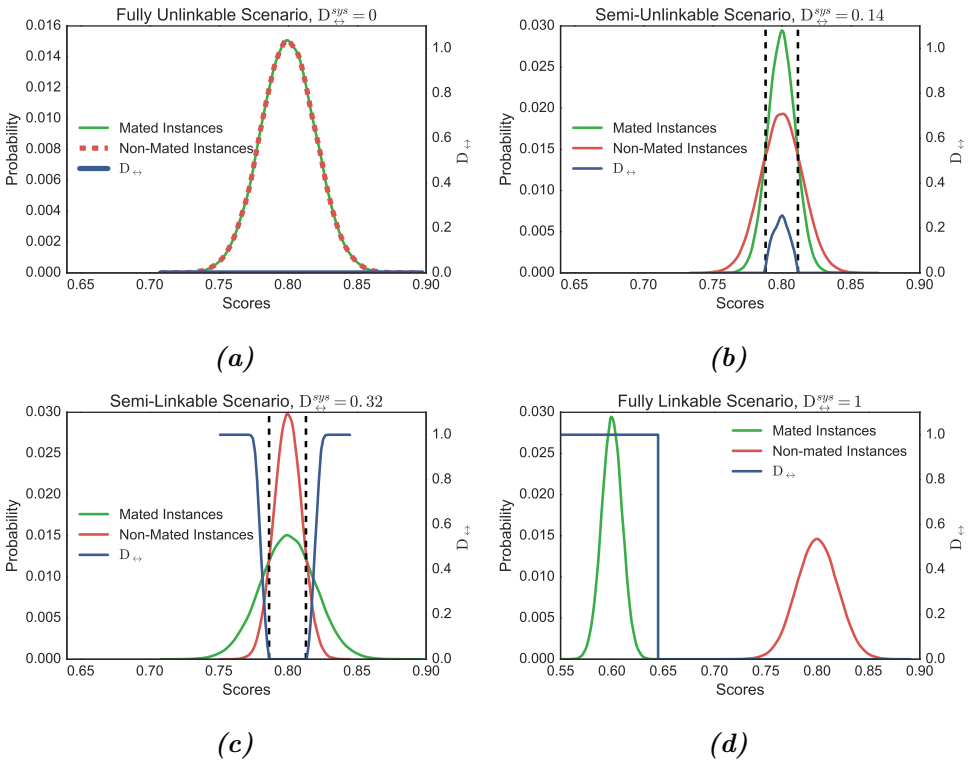


Figure 3.1: *Examples of Mated instances (green) and Non-mated instances (red) distibutions yielded by (a) fully unlinkable, (b) semi-unlinkable, (c) semi-linkable, and (d) fully linkable templates. While the blue curve represents the proposed unlinkability measure* $D_{\leftrightarrow}(s)$ *for each possible score value,* $D_{\leftrightarrow}^{sys}$ *gives an estimation of the unlinkability level of the whole system independently of the score range. The dashed black lines represent* $LR(s) = 1$.

Traditionally, in order to compare the aforementioned distributions, the difference between probability densities has been estimated in terms of the Kullback-Leibler (KL) divergence [Kullback and Leibler, 1951] between two discrete distributions, P and Q, which is defined as:

$$D_{KL}(P||Q) = \sum_i P(i) \ln\left(\frac{P(i)}{Q(i)}\right) \tag{3.5}$$

where $D_{KL} \geq 0$, and $D_{KL} = 0$ holds iff $P \simeq Q$, i.e. the smaller D_{KL}, the higher the similarity between distributions.

However, this measure is not appropriate due to three main reasons: *i*) it gives only an overall measure of the unlinkability of the system, not being possible to measure the level of unlinkability for different ranges of the similarity scores, *ii*) it is not bounded, thus making it difficult to compare the unlinkability of different systems, and *iii*) it is not defined for $Q(s) = 0$ if $P(s) \neq 0$, hence not taking into account important ranges of scores, or not being at all defined for fully separable distributions.

As a consequence, we need a new framework to evaluate the degree of unlinkability of such scenarios. To that end, we propose two different measures: $D_{\leftrightarrow}^{sys}$ and $D_{\leftrightarrow}(s)$:

- On the one hand, $D_{\leftrightarrow}^{sys} \in [0, 1]$ gives an estimation of the linkability of a system as a whole,

independently of the score. Accordingly, this metric is appropriate for example to compare the unlinkability level of two systems as a whole. This way, if a system has $\mathrm{D}_{\leftrightarrow}^{sys} = 1$ (i.e., case in which both the *Mated instances* and *Non-mated instances* distributions have no overlap, as shown in Fig. 3.1d), it means that it is fully linkable in all its score range. That is, if a cross-matching attack is carried out on the system between two protected templates $\mathbf{C}^1$ and $\mathbf{C}^2$, independently of the score produced, the attacker can know (with almost all certainty) if they conceal or not to same instance. Similarly, $\mathrm{D}_{\leftrightarrow}^{sys} = 0$ (i.e., Fig. 3.1a, where both score distributions totally overlap) means that the system is fully unlinkable for the whole score range. That is, independently of the score produced in a cross-matching attack, it is equally probable that the two templates come from the same instance (H_m) than from different instances (H_{nm}). All intermediate values of $\mathrm{D}_{\leftrightarrow}^{sys}$ between 0 and 1 report a decreasing degree of unlinkability (i.e., increasing degree of linkability).

- On the other hand, $\mathrm{D}_{\leftrightarrow}(s) \in [0, 1]$ gives an estimation of the linkability of a system for a *specific score*. As such, this metric is appropriate to analyse within one system in which parts of the score range it fails to provide unlinkability. This way, if for a specific score s_0, a system yields $\mathrm{D}_{\leftrightarrow}(s_0) = 1$, it means that, *in case* a cross-matching attack produced s_0, the attacker would be able to link both templates $\mathbf{C}^1$ and $\mathbf{C}^2$ to the same user with almost all certainty. On the other hand, $\mathrm{D}_{\leftrightarrow}(s_0) = 0$ should be interpreted as full unlinkability for that particular score. In other words, *if* s_0 were produced in a cross-matching attack, the probability that both templates came from the same instance or from different instances would be the same. All intermediate values of $\mathrm{D}_{\leftrightarrow}(s)$ between 0 and 1 report a decreasing degree of unlinkability (i.e., increasing degree of linkability).

It should be noted that both measures yield values in a closed range, in opposition to D_{KL}, in order to allow a more straightforward comparison of different schemes. Next, we describe how both metrics, $\mathrm{D}_{\leftrightarrow}(s)$ and $\mathrm{D}_{\leftrightarrow}^{sys}$, are computed. Furthermore, to illustrate the different levels of unlinkability that templates can achieve, four different scenarios are shown in Fig. 3.1, where the *Mated instances* distribution is depicted in green and the *Non-mated instances* distribution in red, and the newly proposed $\mathrm{D}_{\leftrightarrow}(s)$ in blue:

- A fully unlinkable scenario is shown in Fig. 3.1a, where both distributions are identical. In this case, no decision can be made on whether, for a given score, the templates protect the same identity.

- A semi-unlinkable scenario is shown in Fig. 3.1b, where the *Mated instances* distribution is enclosed within the *Non-mated instances* curve. As we may observe, for score values in $[0.79, 0.81]$ we can state with some certainty that both templates are more likely to belong to the same instance. On the other hand, if the score is out of that range, the attacker can assume that such templates belong to different instances with a higher probability. Similarly, if he were able to compare a protected template with several references enrolled in the system in order to find the template concealing the same identity, he could discard

templates yielding scores out of the aforementioned range and hence reduce the domain of his search.

- A semi-linkable scenario is shown in Fig. 3.1c, where the *Mated instances* distribution spans further than the *Non-mated instances* curve. More specifically, if the score is out of the range $[0.79, 0.81]$, the probability of both templates belonging to different instances is almost zero. As a consequence, we can assume with almost all certainty that both templates protect the same instance, thus making the templates linkable.

- A fully-linkable scenario is shown in Fig. 3.1d, where the *Mated instances* and *Non-mated instances* distributions are fully separable. Therefore, the attacker can make a decision with almost all certainty for all scores.

3.2.2.1. Computation of $\mathrm{D}_{\leftrightarrow}(s)$ and $\mathrm{D}_{\leftrightarrow}^{sys}$

Inspired in the analysis of biometric forensic evidence [Gonzalez-Rodriguez *et al.*, 2006; Morrison, 2011], likelihood ratios can be used to give an estimation of those certainties or unlinkability levels. For a given score s, $LR(s)$ is defined as

$$LR(s) = \frac{p(s|H_m)}{p(s|H_{nm})} \tag{3.6}$$

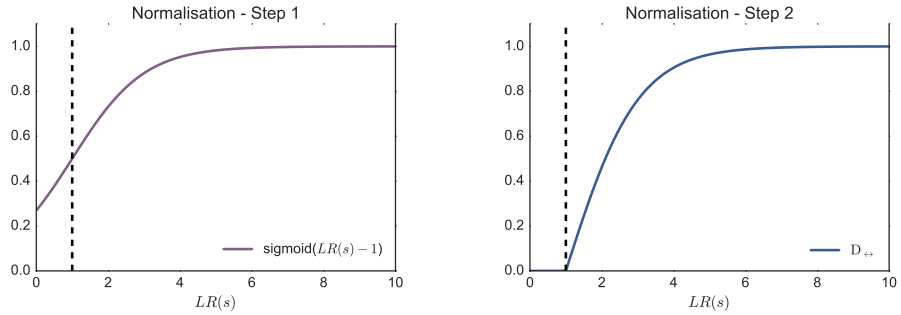
In particular, two different cases can be defined based on $LR(s)$:

- If $LR(s) \leq 1$, we can state that it is more likely that both templates belong to non-mated instances, thereby making the templates unlinkable for those score values. Therefore, we will have $\mathrm{D}_{\leftrightarrow}(s) = 0$.

  Bear in mind that a system is considered to be linkable if it allows determining, with some certainty, that two templates come from the same person. In the case of $LR(s) \leq 1$, a potential attacker knows, with some certainty, that both templates do *not* belong to the same subject and therefore he cannot link them. That is why for those score values the system is considered to be unlinkable, i.e., $\mathrm{D}_{\leftrightarrow}(s) = 0$.

- If $LR(s) > 1$, we can state that it is more likely that both templates belong to the same instance, thereby making the templates somewhat linkable for those score values. In fact, the higher $LR(s)$, the more linkable the templates are. As a consequence, we will define an increasing value $\mathrm{D}_{\leftrightarrow}(s) \in (0, 1]$, with higher values for more linkable templates (i.e., the higher $LR(s)$, the closer $\mathrm{D}_{\leftrightarrow}(s)$ to 1).

Keeping those remarks in mind, we define $\mathrm{D}_{\leftrightarrow}(s)$ as a function of s and its corresponding $LR(s)$. Since $LR(s)$ yields values in the range $[0, \infty)$, in order to obtain the desired measure in the range $[0, 1]$, we perform a two step normalisation, as depicted in Fig. 3.2. In the first step (Fig. 3.2a), we normalise $LR(s) - 1$ to the range $[0.5, 1]$ with a sigmoid function. Then,



(a) *(b)*

Figure 3.2: *Two step normalisation followed to obtain the final unlinkability metric* $D_{\leftrightarrow}(s)$*: (a) LR values in* $[1, \infty)$ *are normalised to the range* $[0.5, 1]$ *with a sigmoid function, and (b) the interval* $[0.5, 1]$ *is mapped to the interval* $[0, 1]$ *to obtain the final* $D_{\leftrightarrow}$*. The dashed black line represents the point at which* $LR(s) = 1$*.*

we subtract 0.5 and multiply by 2 to map that interval to $[0, 1]$ (Fig. 3.2b). Therefore, we can finally define $D_{\leftrightarrow}(s)$ as

$$D_{\leftrightarrow}(s) = \begin{cases} 0 & \text{if } LR(s) \leq 1 \\ 2 \cdot \left(\left(1 + e^{-(LR(s)-1)}\right)^{-1} - 0.5 \right) & \text{if } LR(s) > 1 \end{cases} \tag{3.7}$$

As it was previously described, it is also useful to have an estimation of the *unlinkability of the whole system* (and not for every single score). For this purpose, we define $D_{\leftrightarrow}^{sys}$ as the partial area under the curve $D_{\leftrightarrow}(s)$, normalised by $p(s|H_m)$ in order to get values in $[0, 1]$, and computed on the whole score range (i.e., $[s_{min}, s_{max}]$):

$$D_{\leftrightarrow}^{sys} = \int_{s_{min}}^{s_{max}} D_{\leftrightarrow}(s) \cdot p(s|H_m)\, ds \tag{3.8}$$

This way, the final value of $D_{\leftrightarrow}^{sys}$ depends on: *i*) the range of scores where the system is linkable; *ii*) how linkable the system is in that range of scores; and *iii*) how probable it is that such scores are produced.

Let us now evaluate the scenarios shown in Fig. 3.1 with the proposed measures:

- For the fully unlinkable scenario shown in Fig. 3.1a, $D_{\leftrightarrow}(s) = 0$ for all scores, thus yielding the desired value $D_{\leftrightarrow}^{sys} = 0$.

- For the semi-unlinkable scenario shown in Fig. 3.1b, we may observe that $D_{\leftrightarrow}(s) = 0$ for all scores where H_{nm} holds (i.e., $s \notin [0.79, 0.81]$). Additionally, $D_{\leftrightarrow}(s)$ reaches a maximum of 0.2 for a score value of 0, where the LR is the highest ($LR(0) \sim 1.5$) and we can thus assume with the highest certainty that both templates conceal the same identity. Overall, we obtain $D_{\leftrightarrow}^{sys} = 0.14$, reflecting the fact that only for a small range of scores we could link templates.

- For the semi-linkable scenario shown in Fig. 3.1c, we observe that $\mathrm{D}_{\leftrightarrow}(s) = 1$ for scores out of $[0.79, 0.81]$, where $p(s|H_{nm}) = 0$, and we can assume with almost all certainty that the compared templates conceal the same instance. As a consequence, we obtain a higher value for $\mathrm{D}_{\leftrightarrow}^{sys} = 0.32$, with respect to the semi-unlinkable scenario.
- For the fully linkable scenario shown in Fig. 3.1d, we observe that $\mathrm{D}_{\leftrightarrow}(s) = 1$ where only the *Mated instances* distribution is non-null (i.e., $s \in [0.55, 0.65]$), since templates are fully linkable in such range. On the other hand, $\mathrm{D}_{\leftrightarrow}(s) = 0$ in any other place. Therefore the system as a whole is fully linkable, as it holds that $\mathrm{D}_{\leftrightarrow}^{sys} = 1$, as desired.

Finally, it should be noted that such unlinkability analysis is not sufficient to ensure the cross-matching resistance of protected templates, since the robustness against specifically designed attacks has to be analysed as well [Simoens *et al.*, 2012b]. To that end, the aforementioned distributions will be estimated not only for the dissimilarity scores computed by the biometric system, but also for other appropriate distance measures for the cross-matching attack at hand (e.g., Hamming Distance, Hamming Weight difference), and analysed in the same manner.

3.2.3. Accuracy Analysis

As defined in Sect. 3.2.1, during irreversibility analyses of *unprotected templates*, defining the operating points of the system will enable to compare, in a more fair manner, the vulnerabilities of different systems to the same inverse biometrics attack (i.e., we can determine for a given FMR or FNMR which of them is less/more robust to the attacking approach). To that end, we need to evaluate the accuracy of the unprotected biometric system following the guidelines established in Sect. 3.1:

- Define which mated and non-mated comparison trials will be issued.
- Compute the operating points at which the inverse biometrics attack will be carried out.

Secondly, in the case a *BTP algorithm* is integrated in the system, the first question to analyse is the impact of the proposed improvements on the biometric accuracy of the baseline unprotected system. Therefore, the accuracy of the baseline unprotected biometric system and that of the proposed BTP are evaluated on the same standardized database, following a common protocol. According to Sect. 3.1, the main parameters of each system should be reported, namely: EER, FNMR at specific FMRs and DET curves. Only that way can we establish a fair comparison between both scenarios (i.e., unprotected and protected) and evaluate the accuracy degradation (if any). As a consequence, a three-step protocol will be followed:

- Define a common accuracy analysis protocol for both scenarios: which mated and non-mated comparison trials will be issued.
- Analyse the accuracy of the baseline unprotected system.
- Analyse the accuracy of the BTP system.

- Assess the accuracy degradation comparing the results of both analyses.

3.3. Biometric Verification Systems

As defined at the beginning of Sect. 3.2, the first step in the proposed methodology for the security and privacy evaluation of biometric systems is to define the biometric systems used for the accuracy, irreversibility and unlinkablity analyses. In this section, we present the unprotected biometric systems analysed in Chapter 4 and then protected with Bloom filters in Chapter 5 and with Homomorphic Encryption in Chapter 6. All systems are publicly available, well described in the literature or commercial, in order to ensure reproducible research.

3.3.1. Hand Verification

In order to ensure unbiased results, and fully analyse the vulnerabilities of hand-based systems to the new inverse-biometric method proposed in Chapter 4, four different systems will be evaluated. The first one is used for the development experiments, and the last three systems at the validation stage.

3.3.1.1. Geometry-based system I

Ferrer and Morales [2011] compute geometric features of the hands (48 widths and 4 lengths from the little, ring, middle and index fingers) by measuring the widths and lengths of each finger. For verification, a least squares support vector machine (LS-SVM) is used to model each hand [Suykens *et al.*, 2002; Yen *et al.*, 2013]. This system does not take into account any features obtained from the thumb as, due to their high variability, it has been demonstrated that they do not improve the accuracy of the geometry-based hand recognition systems [Duta, 2009].

3.3.1.2. Geometry-based system II

Burgues *et al.* [2009] take measures of the four fingers (excluding the thumb) lengths and widths. Then, the Manhattan distance between hand feature vectors is used as dissimilarity measure.

3.3.1.3. Appearance-based system

Yörük *et al.* [2006] propose a system which makes its decisions based on the whole hand shape, including the thumb, considering independent component features (ICA2) and images normalized after pose correction.

3.3.1.4. Silhouette-based system

Ferrer and Morales [2011] present a new method based on direct silhouette alignment of 50 equal spaced samples of the finger contour of the hands, excluding the thumb. The matching

score is computed estimating the modified Hausdorff distance between the silhouettes of the fingers of two hands after an alignment that includes translation and rotation with no shape deformation.

3.3.2. Iris Verification

The vulnerabilities of iris templates, or iriscodes, to inverse biometrics methods are analysed in Chapter 4, using two different systems in order to ensure unbiased results. Afterwards, in Chapter 5, Bloom filter template protection is applied to iris verification.

3.3.2.1. LogGabor filter-based

This system is used in Chapter 4 for the development experiments. In this particular implementation of Masek's matcher [Masek and Kovesi, 2003][1], the different stages involved in iris recognition are implemented following a *classical* approach: *i*) for *segmentation*, the method proposed in [Ruiz-Albacete *et al.*, 2008] is followed, modelling the iris and pupil boundaries as circles; *ii*) for *normalization*, a technique based on Daugman's rubber sheet model that maps the segmented iris region into a 2D array is used [Daugman, 2004]; *iii*) *feature encoding* produces a binary template of $20 \times 480 = 9,600$ bits by filtering the normalized iris pattern with 1D Log-Gabor wavelets and quantizing the filtered output to four levels (i.e., two bits) according to [Daugman, 2004]; and *iv*) for *matching*, a modified Hamming distance that takes into account the noise mask bits is used.

The particular implementation of this system within the publicly available University of Salzburg Iris Toolkit v1.0[2] [Uhl and Wild, 2012], yielding a higher accuracy, is protected in Chapter 5 with Bloom filters. In this case, the iris texture is divided into 10 stripes to obtain 5 one dimensional signals, each one averaged from the pixels of 5 adjacent rows. A row-wise convolution with a complex Log-Gabor filter is then performed on the texture pixels. The phase angle of the resulting complex value for each pixel is discretised into 2 bits, which are subsequently used to generate a binary code comprising $20 \times 512 = 10,240$ bits.

3.3.2.2. VeriEye

For the validation experiments in Chapter 4, the VeriEye [Neurotechnology] commercial matcher marketed by Neurotechnology[3] is used to determine the matching potential of the reconstructed iris images. The motivation for its selection is two-fold: *i*) it was ranked among the top performing matchers in the NIST Iris Exchange (IREX) independent evaluation in 2009 [Grother *et al.*, 2009], and, *ii*) being a commercial matcher it works as a black-box for the subject, who has no knowledge of the algorithms used in any of the stages of the iris recognition process (being a commercial system its implementation details are proprietary).

[1] `www.csse.uwa.edu.au/pk/studentprojects/libor/sourcecode.html`
[2] `http://www.wavelab.at/sources/`
[3] `http://www.neurotechnology.com/verieye.html`

3.3.3. Face Verification

This system is protected in Chapter 5 with Bloom filters. It is an implementation of the Local Gabor Binary Pattern Histogram Sequences (LGBPHS) algorithm [Zhang *et al.*, 2005], a state-of-the-art system robust to illumination changes. In a fair benchmark among four state-of-the-art algorithms for face recognition established in [Günther *et al.*, 2012], using the same databases and protocols, LGBPHS achieved a top accuracy. Feature extraction is applied in a block-wise manner, i.e. the facial image is divided into 80 non-overlapping sub-images, from which spectral histograms are computed and concatenated to form the final template.

In the Dissertation, we have used the implementation within Bob[1] [Anjos *et al.*, 2012], a free signal and image processing toolbox, which includes a library with implementations of several face verification algorithms - the Facereclib [Günther *et al.*, 2012]. Furthermore, out of the total 80 sub-images, we have considered only the central 32 sub-images for verification purposes.

3.3.4. Fingervein Verification

The unprotected biometric system proposed in [Raghavendra *et al.*, 2014], which outperforms other fingervein verification systems in the state-of-the-art, is protected in Chapter 5 with Bloom filters. In this particular approach, the Region of Interest (ROI) is segmented following the method described in [Raghavendra *et al.*, 2013]: images are rotated according to the angle between the central axis [Huang *et al.*, 2010] and the image reference axis, in order to obtain alignment-free templates, and the ROI is extracted based on the detected fingertip point. Then, ROI images are enhanced using adaptive histogram equalization [Zuiderveld, 1994] before applying the maximum curvature method presented in [Miura *et al.*, 2007] to extract the connected vein pattern. In the original approach, two successive steps were followed: the minutiae points are determined based on convolution filters according to the algorithm described in [Olsen *et al.*, 2011] and finally, the real-valued Spectral Minutiae Representation (SMR) [Xu *et al.*, 2009a] is extracted. Then, as proposed in [Xu *et al.*, 2009b], in order to reduce the dimensionality of the template, column-PCA is applied to the SMR, and only the top 18 rows are retained. Finally, the Hamming Distance is used to compute similarity scores.

3.3.5. Fingerprint Verification

3.3.5.1. Variable-Length Fingerprint Verification

This system, based on minutiae vicinities, is protected in Chapter 5 with Bloom filters. In the first step, minutiae are extracted with the Neurotechnology VeriFinger SDK 6.0 [2], and only those minutiae in the neighbourhoods of the core points are considered. Binary templates of size $256 \times nVicinities$ are generated following the method proposed in [Yang *et al.*, 2010], where each column represents one minutiae vicinity [Yang and Busch, 2009], comprising a central minutia

[1] `http://idiap.github.io/bob/`

[2] `http://www.neurotechnology.com/verifinger.html`

and its three closest neighbouring minutiae. From each vicinity, a 36 dimensional vector is generated with the x and y coordinates, as well as the angle information, of all the possible minutiae pairs within the vicinity. Finally, this vector is projected to a $36 \times 16 = 576$ binary string, which is further downsized to an 256 binary vector. Templates are then compared in a vicinity-wise way, minimizing the Hausdorff distance between corresponding vicinities.

3.3.5.2. Fixed-Length Fingerprint Verification

This system is protected in Chapter 6 with Homomorphic Encryption. In the FingerCode scheme presented in [Jain *et al.*, 1999], a region of interest is located and divided into 80 sectors. These sectors are filtered with eight Gabor filters, and the final template comprises the standard deviations of the grey values comprised by each sector for each filter. From the original $80 \times 8 = 640$ features, a subset of the best performing 100 has been selected with the method proposed in [Maiorana *et al.*, 2009]. Similarity scores are computed using the Euclidean distance, with no specific pre-alignment between samples.

3.3.6. On-Line Signature Verification

Two different systems are protected in Chapter 6 with Homomorphic Encryption, the former based on variable-length templates and the later on fixed-length templates.

3.3.6.1. Variable-Length Signature Verification

Martinez-Diaz *et al.* [2014] propose the use of a subset of $F = 9$ time sequences selected using the Sequential Forward Floating Selection (SFFS) algorithm from the total set of functions defined in [Martinez-Diaz *et al.*, 2014]. Those time sequences, which include, for instance, the horizontal and vertical coordinates, the speed or the pressure, are directly compared using DTW [Kholmatov and Yanikoglu, 2005].

In particular, in order to obtain a dissimilarity score between the probe and the reference templates, a cost matrix is computed, minimizing the distance between signature points in terms of their Euclidean distance. To reduce complexity, only three directions are considered at each step. The final dissimilarity score is the last cell of the matrix.

For a more detailed description of the use of DTW for on-line signature verification the interested reader is referred to [Kholmatov and Yanikoglu, 2005; Martinez-Diaz *et al.*, 2014].

3.3.6.2. Fixed-Length Signature Verification

In this system, signatures are parametrized using the set of features described in [Martinez-Diaz *et al.*, 2014], which include information such as the total duration of the signature, the number of pen-ups or the average speed. In that work, a set of 100 global features was proposed, and the individual features were ranked according to their individual discriminant power. A good operating point for the systems tested was found when using the first 40 parameters. In the

present contribution we use this 40-feature representation of the signatures, normalizing each of them to the range [0,1] using the tanh-estimators described in [Jain *et al.*, 2005].

The similarity scores are computed using the Mahalanobis distance between the input vector and a statistical model of the attacked client, using a number of enrolment signatures (4 or 5 in our experiments).

3.4. Biometric Databases

As defined at the beginning of Sect. 3.2, the second step in the proposed methodology for the security and privacy evaluation of biometric systems is to define the databases used for the accuracy, irreversibility and unlinkablity analyses. In this section, we present the biometric databases used in the experiments in Chapters 4, 5 and 6. References to the evaluations where they have been used are also included. All databases are publicly available in order to ensure reproducible research.

3.4.1. Hand Biometric Databases

In Chapter 4, the security and privacy of hand-based templates is analysed. To that end, several databases are used to ensure unbiased results.

3.4.1.1. GPDS Hand Database

The first set of images reconstructed in Sect. 4.2.1 come from the GPDS[1] dataset [Ferrer *et al.*, 2007], which comprises 144 subjects with 10 images per subject (only right hand of each subject, $144 \times 10 = 1,440$ hand images). All of them were acquired in one session with a commercial digital scanner of 150 dpi at the University of Las Palmas de Gran Canaria, placing the right hand flat on the glass platen.

3.4.1.2. GPDS2 Hand Database

In order to train the required parameters, in Sect. 4.2.1 the GPDS2 database [Morales *et al.*, 2012] is used. It comprises one sample of the right hand of 100 subjects (100 hand images), captured with a 60 dpi commercial scanner in one session. It should be noted that with such resolution (60 dpi) the hand shape is not very accurately defined.

3.4.1.3. UST Hand Database

The second database used in the validation experiments in Sect 4.2.1 is the UST database [The Hong Kong University of Science and Technology, Department of Computer Science]. It comprises 564 instances (right and left hands belonging to the same person are regarded as different identities) with 10 images per instance ($564 \times 10 = 5640$ hand images). Images were

[1] `http://www.gpds.ulpgc.es/download/index.htm`

captured using a CCD camera (1280 × 960 pixels) by the Hong Kong University of Science and Technology. The final version of this database has not been published yet and includes a small number of duplicates.

3.4.2. XM2VTS Face Database

In Chapter 5, the Bloom Filter based template protection scheme proposed in the present Dissertation is applied to face data. The experimental evaluation for this particular case study is run on the Extended M2VTS multimodal face Database[1] [Messer *et al.*, 1999]. For the experiments, a subset of the entire videos, captured with a Sony VX1000E digital cam-corder and DHR1000UX digital VCRF, comprising four frontal images from each of the 295 subjects was selected ($295 \times 4 = 1,180$ face images).

3.4.3. IITD Iris Database

In Chapter 5, the Bloom Filter based template protection scheme is applied to iris data. The widely used IIT Delhi Iris Database version 1.0[2] [Kumar and Passi, 2010] is used for the accuracy analysis. It comprises five NIR images from 224 different subjects, captured with a JIRIS JPC1000 digital CMOS camera ($224 \times 5 = 1120$ iris images).

3.4.4. FVC2002 Fingerprint Database

In Chapter 5, the Bloom Filter based template protection scheme is applied to fingerprint data. The DB2A subset of FVC 2002[3] [Maio *et al.*, 2002a] is used for the accuracy analysis. This subset includes eight samples of 100 fingers ($100 \times 8 = 800$ fingerprint samples), acquired with the Biometrika FX2000 optical sensor.

3.4.5. Fingervein Biometric Databases

In Chapter 5, the Bloom Filter based template protection scheme is applied to fingervein data. Two different databases are used for the development experiments and the final analysis.

3.4.5.1. UTFVP Fingervein Database

For fingervein, development experiments are performed on the UTFVP database[4] [Ton and Veldhuis, 2013], which was captured with a specific device designed at the University of Twente. The database comprises data from 60 different subjects, from whom the vascular pattern of the index, ring and middle finger of both hands was collected twice at each of the two acquisition sessions ($60 \times 6 \times 4 = 1,440$ fingervein samples).

[1] `http://www.ee.surrey.ac.uk/CVSSP/xm2vtsdb/`
[2] `http://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm`
[3] `http://bias.csr.unibo.it/fvc2002/databases.asp`
[4] `http://www.sas.el.utwente.nl/home/datasets`

3.4.5.2. SDUMLA-HMT Fingervein Subset

The SDMULA-HMT multimodal database[1] [Yin *et al.*, 2011], used in the accuracy analysis, comprises fingervein, gait, iris and fingerprint data from 106 subjects. The fingervein subset was acquired with a device designed at the Wuhan University, capturing six images of each subject's index, middle and ring fingers of both hands. Therefore, the database comprises a total number of $106 \times 6 \times 6 = 3,816$ fingervein samples, belonging to $106 \times 6 = 636$ different identities.

3.4.6. Multimodal Biometric Databases

Two different multimodal databases have been used in Chapters 4, 5 and Chapter 6.

3.4.6.1. Biosecure Multimodal Biometric Database

The Desktop Dataset of the Multimodal Biosecure database[2] [Ortega-Garcia *et al.*, 2010] comprises voice, fingerprints, face, iris, signature and hand samples of 210 subjects, captured in two timespaced acquisition sessions. The face subset includes four frontal images (two per session) with an homogeneous grey background, captured with a reflex digital camera without flash ($210 \times 4 = 840$ face samples). Eyes were automatically annotated using VeriLook SDK 4.0, developed by Neurotechnology[3]. The iris subset includes four samples (two per session) acquired with the LG Iris Access EOU3000 infrared sensor ($210 \times 4 = 840$ iris samples). Finally, four fingerprint samples (two per session) of the thumb, index and middle fingers of each hand were captured with the Biometrika FX2000 optical sensor ($210 \times 3 \times 2 \times 4 = 5,040$ fingerprint samples, belonging to $210 \times 3 \times 2 = 1,260$ different identities). These subsets are used in Chapter 5 for the development experiments.

Additionally, in Chapter 4, irides were reconstructed.

3.4.6.2. BiosecurID Multimodal Biometric Database

Very few multimodal databases including on-line signature data are available. Among them, BiosecurID DB [Fierrez *et al.*, 2009] is one of the most recently acquired, comprising fingerprint, signature, face, hand, iris and speech data belonging to 400 subjects. All samples were acquired in four time-spanned sessions at six different sites in an office-like uncontrolled environment simulating a realistic scenario.

For the on-line signature subset, four genuine signatures were captured in each session with the Wacom Intuos3 A4 Inking Pen Tablet, thus yielding $400 \times 4 \times 4 = 6,400$ genuine signatures. The fingerprint subset comprises data of four fingers per subject, captured with a thermal and an optical sensor (Biometrika FX2000). For the present study, only the right index acquired with the optical sensor has been considered, therefore having $400 \times 4 \times 4 = 6,400$ fingerprint samples. These subsets are protected in Chapter 6 with Homomorphic Encryption.

[1] `http://mla.sdu.edu.cn/sdumla-hmt.html`

[2] `http://biosecure.it-sudparis.eu/AB`

[3] `http://www.neurotechnology.com/verilook.html`

3.5. Chapter Summary and Conclusions

In this chapter we have outlined some best practices for accuracy analysis in biometric authentication. We have also provided a description of the security and privacy evaluation protocol followed in this Thesis to assess both unprotected and protected biometric systems, which can serve as guideline to carry out systematic and replicable security and privacy studies. Finally we have described the databases and unprotected biometric systems used in this Thesis.

This chapter includes novel contributions in:

- Proposal of a systematic protocol for security and privacy evaluation of unprotected and protected biometric templates, in order to assess whether BTP schemes fulfil the requirements established in the ISO/IEC IS 24745 on biometric information protection [ISO/IEC JTC1 SC27 IT Security Techniques, 2011].
- New framework for the unlinkability analysis of biometric templates.

Chapter 4

Inverse Biometrics Attacks to Unprotected Biometric Templates

In this Chapter, we propose two new inverse biometrics methods based on optimization algorithms to analyse the security and privacy offered by unprotected biometric systems, according to the protocol described in Chapter 3, Sect. 3.2. In particular, the irreversibility of unprotected templates will be analysed with the aforementioned methods. Their aim is to reconstruct a set of biometric samples from the information stored in the unprotected template. The reconstructed samples, due to the probabilistic nature of the optimization algorithms, will be different to each other. However, all of them will positively match the reference template, thereby posing a threat to the subject's privacy. Such threat is analysed launching attacks to different biometric systems.

Two different methods are proposed:

- Novel inverse biometric algorithm for the reconstruction of handshape samples, based on a combination of a handshape images generator and the uphill simplex integer optimization algorithm.
- Novel inverse biometric algorithm for the reconstruction of iris samples, based on a genetic algorithm for the optimization of real valued matrices.

The chapter is structured as follows. Sect. 4.1 estates the problem to be solved with the aforementioned inverse biometric methods, which are described in detail in Sects. 4.1.1 and 4.1.2. The privacy threat posed by those schemes is evaluated in Sect. 4.2 following a common protocol, and results for each case study are given in Sect. 4.2.1 and 4.2.2, respectively. Finally, Sect. 4.3 summarises and concludes the chapter.

This chapter is based on the publications: [Galbally *et al.*, 2013; Gomez-Barrero *et al.*, 2014b, 2012a].

We will use the following notation throughout the chapter:

- **I**: real biometric image that we want to reconstruct.

- $\mathbf{T}$: unprotected template extracted from a real biometric image and stored in the database.
- $\mathbf{I_R}$: reconstructed synthetic image.
- $\mathbf{T_R}$: template associated to $\mathbf{I_R}$.
- $\mathcal{F}$: function that extracts an unprotected template, given a biometric sample, i.e., $\mathbf{T} = \mathcal{F}(\mathbf{I})$.
- $\mathcal{J}$: function that computes the similarity score between two templates, i.e., $\mathcal{J}(\mathbf{T}_1, \mathbf{T}_2)$.
- $\mathcal{V}$: function that computes the similarity score between the reference template and the reconstructed image, i.e., $\mathcal{V}(\mathbf{T}, \mathbf{I_R}) = \mathcal{J}(\mathbf{T}, \mathcal{F}(\mathbf{I_R})) = \mathcal{J}(\mathbf{T}, \mathbf{T_R})$.

4.1. Inverse Biometrics Based on Optimization Algorithms

According to the security and privacy evaluation methodology presented in Chapter 3, Sect. 3.2, one of the key steps in the evaluation is the irreversibility analysis of the templates. To perform such assessment, in this section we present two new methodologies for the reconstruction of biometric samples. In addition to the description of the systems and databases used in the evaluation, the aforementioned protocol requires the definition of: *i*) the assumed knowledge for the attacker and *ii*) the experimental protocol (i.e., problem or challenge to be solved and algorithms to solve it). We will do so in the following.

Problem statement. Consider the problem of finding an $\mathbf{I_R}$ matrix such that, its associated $\mathbf{T_R} = \mathcal{F}(\mathbf{I_R})$ matrix (unknown), produces a similarity score (s) greater than a certain threshold δ, when it is compared to a *known* binary matrix $\mathbf{T}$ according to some unknown matching function $\mathcal{J}$, i.e., $\mathcal{J}(\mathbf{T}, \mathbf{T_R}) > \delta$. For clarity, we will define a new function $\mathcal{V}$ as: $s = \mathcal{V}(\mathbf{T}, \mathbf{I_R}) = \mathcal{J}(\mathbf{T}, \mathcal{F}(\mathbf{T_R}))$.

Assumed Knowledge. Let us assume that we have access to the evaluation of the function $\mathcal{V}(\mathbf{T}, \mathbf{I_R})$ for several trials of $\mathbf{I_R}$.

Algorithm. In the next subsections, we will propose two different algorithms for the reconstruction of hand shape (Sect. 4.2.1) and iris samples or images (Sect. 4.2.2).

The reconstruction methods proposed share some characteristics:

- Due to the probabilistic nature of the optimization algorithms (either the uphill simplex initialization - step 2: *random* sampling of the statistical model G - or the four rules applied by the genetic algorithm), the methods produce different solutions at each execution. This permits the reconstruction of more than one sample ($\mathbf{I_R}$) with very similar templates ($\mathbf{T_R}$) to the target ($\mathbf{T}$).
- Furthermore, the algorithms do not require any information about:
  - The mapping function $\mathcal{F}$ between the reconstructed biometric samples ($\mathbf{I_R}$) and their corresponding templates ($\mathbf{T_R}$).

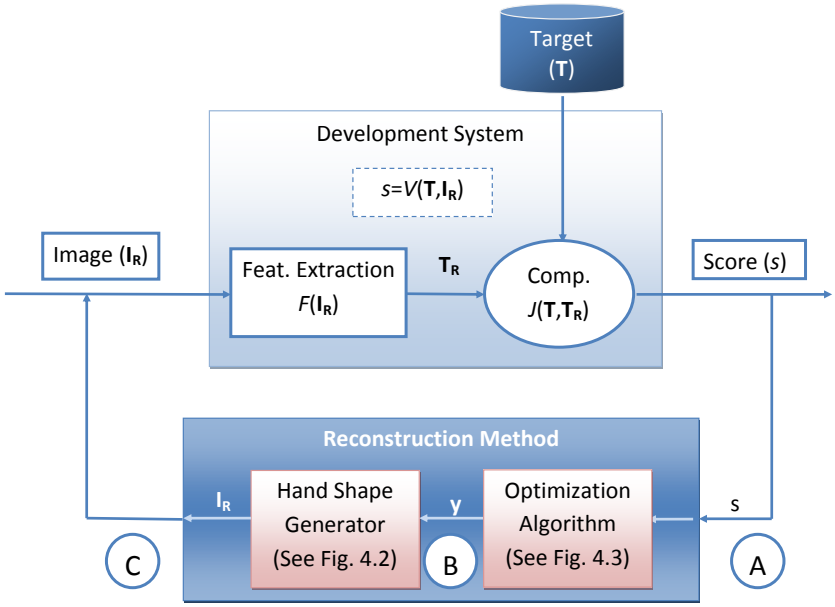


Figure 4.1: General diagram of the hand shape reconstruction method. *A detailed diagram of the reconstruction approach is given in Figs. 4.2 and 4.3, where points A, B and C show, respectively, the input and output of the algorithms.*

- The matching function $\mathcal{J}$.
- The function $\mathcal{V}$, only needing access to its outcome for given inputs.

4.1.1. Attacking Handshape Templates: Inverse Biometrics Based on the Uphill Simplex Algorithm

In the case of biometric systems based on handshape, the problem stated above may be solved combining the hill-climbing approach based on the Uphill Simplex algorithm first presented in [Gomez-Barrero *et al.*, 2011] to optimize the input of a generator of hand shape images, according to the general diagram presented in Fig. 4.1.

Handshape generator. The generator used to obtain the matrices $\mathbf{I_R}$ (hand shape images) that will be compared with the reference template target, $\mathbf{T}$, is based on the Active Shape Model approach [Cootes *et al.*, 2001, 1995]. A general diagram of the generator is shown in Fig. 4.2. The first step is to train the ASM model using the aligned hand contours from the development set. The process of aligning the contours can be divided in four stages: *i*) for each hand image, we automatically locate 14 landmarks (see crosses in Fig. 4.2) using the methodology proposed in [Ferrer and Morales, 2011]; *ii*) the contours are aligned by placing the hand geometric center as the coordinate origin, and rotating the hand contour by an angle equal to the slope of the line between the 1st and 3rd finger-web: this allows to reduce the effects of translation and rotation; *iii*) the envelope line between landmarks is sampled with a number of points equal to the average envelope length in the development set divided by five; *iv*) finally, the hand contour

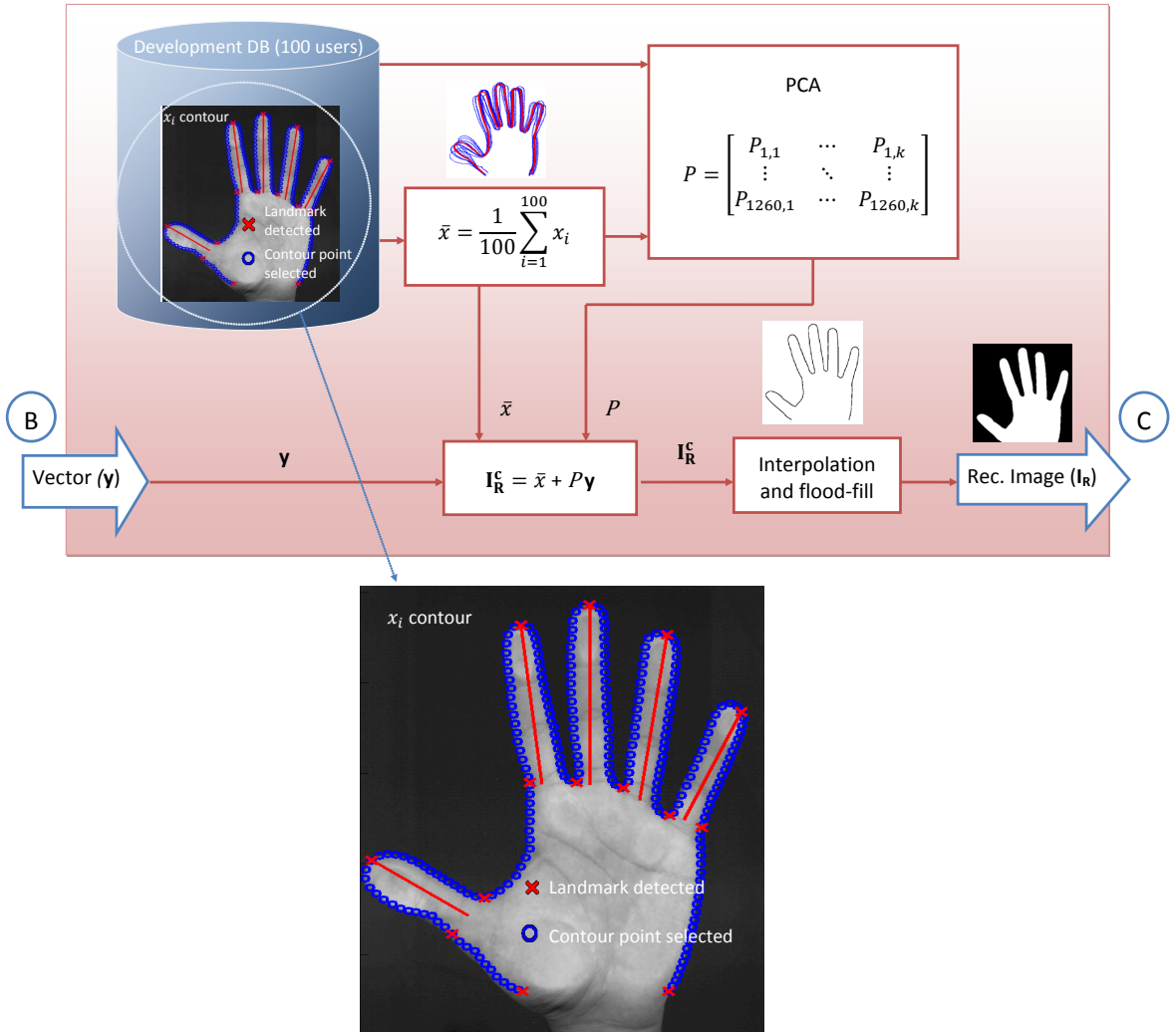


Figure 4.2: General diagram of the hand shape generator *used in the hand shape reconstruction method, with a zoom on the hand landmarks and contour. Points B and C (input and output of the hand shape generator respectively) may be seen for reference in Fig. 4.1.*

is represented as a $2n$ element vector composed by the coordinates (x and y) of $n = 630$ selected contour points.

As we enforce a common number of points between landmarks, the alignment in the positioning of landmarks inside the sampled vector is ensured for all the contours.

Let $\bar{x}$ be the hand mean contour obtained as $\bar{x} = \frac{1}{100}\sum_{i=1}^{100} x_i$, being $x_i \in \mathbb{R}^{2n\times 1}$ the vector that represents the contour of the i-th development subject. Principal Component Analysis (PCA) is applied to determine the k main directions of variation of the development set. A reconstructed hand-contour can be then generated as:

$$\mathbf{I_R^c} = \bar{x} + P\mathbf{y} \tag{4.1}$$

where $P \in \mathbb{R}^{2n\times k}$ is the projection matrix, whose columns are the eigenvectors of the covariance matrix, and $\mathbf{y} = [y_0, \ldots, y_{k-1}]$ is the vector of parameters defining the handshape contour,

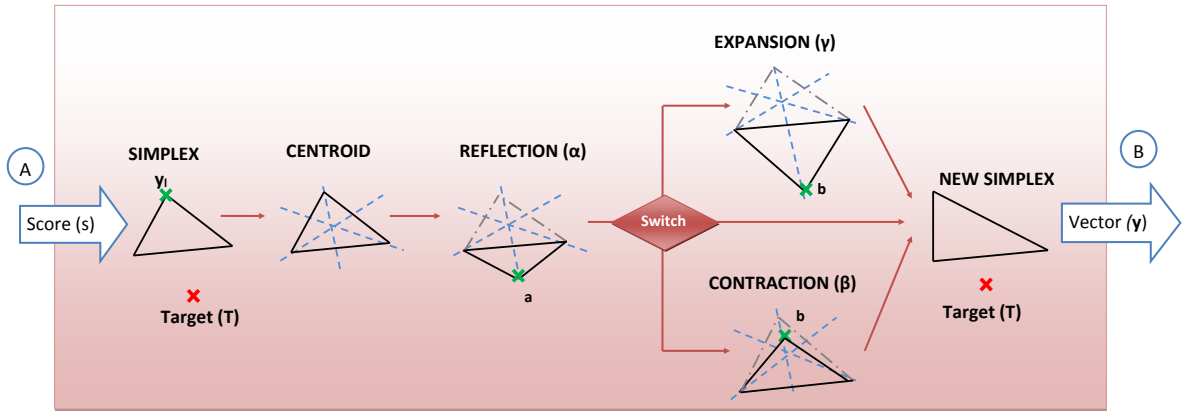


Figure 4.3: Diagram of the probabilistic method *proposed in the present work for the reconstruction of hand shape images from their stored templates. Points A and B (input and output of the optimization algorithm respectively) may be seen for reference in Fig. 4.1.*

which will be optimized by the Uphill Simplex (see below). Using that contour vector $\mathbf{I_R^c}$, the reconstructed binary handshape, $\mathbf{I_R}$, is obtained ensuring the continuity of the contour points by linear interpolation and applying a flood-fill operation on background pixels of the binary contour image generated with $\mathbf{I_R^c}$.

Uphill Simplex. In order to optimize the input of the hand shape generator, as depicted in Fig. 4.1, the proposed reconstruction approach uses the Uphill Simplex algorithm [Gomez-Barrero *et al.*, 2011]. Let us consider a simplex, that is, a polygon defined by $k+1$ points $\mathbf{y}_i$ in the k-dimensional space, obtained from randomly sampling a statistical model G (computed from a development pool of subjects). Each of these $\mathbf{y}_i$ k-dimensional points (with $i = 1, \ldots, k+1$) is transformed into a hand shape image $\mathbf{I_R}$ using the hand shape generator (see Fig. 4.2 and Eq. 4.1). We iteratively form new simplices by reflecting one point, $\mathbf{y}_l$, in the hyperplane of the remaining points, in order to increase at each iteration the value of the mapping function $\mathcal{V}(\mathbf{I_R}, \mathbf{T})$. The point to be reflected will always be the one with the lowest score s, since it is, in principle, the one furthest from our objective (see Fig. 4.3). The algorithm stops when one of the $\mathbf{I_R}^i$ images produces a score higher than the threshold δ.

In particular, the different steps followed by the reconstruction algorithm are:

1. Compute empirically the statistical model G from a development pool of subjects.
2. Take randomly $k+1$ samples ($\mathbf{y}_i$, with $i = 1, \ldots, k+1$) from the statistical model G, hence defining the initial simplex, and generate the corresponding matrices $\mathbf{I_R}^i$, using the hand shape generator (see Fig. 4.2, Eq. 4.1).
3. Compute the similarity scores $\mathcal{V}(\mathbf{T}, \mathbf{I_R}^i) = s_i$.
4. Compute the centroid $\bar{\mathbf{y}}$ of the simplex as the average of $\mathbf{y}_i$.
5. Reflect the point $\mathbf{y}_l$ according to the next steps (see Fig. 4.3), where the indices l and h

are defined as:

$$h = \arg\max_i(s_i) \qquad l = \arg\min_i(s_i)$$

a) **Reflection**: Given a constant $\alpha > 0$, the *reflection coefficient*, we compute:

$$\mathbf{y}_a = (1+\alpha)\bar{\mathbf{y}} - \alpha\mathbf{y}_l.$$

Thus, $\mathbf{y}_a$ is on the line between $\mathbf{y}_l$ and $\bar{\mathbf{y}}$, being α the ratio between the distances $[\mathbf{y}_a\bar{\mathbf{y}}]$ and $[\mathbf{y}_l\bar{\mathbf{y}}]$.
Then generate ${\mathbf{I}_\mathbf{R}}^a$ and compute $s_a = \mathcal{V}(\mathbf{T}, {\mathbf{I}_\mathbf{R}}^a)$. If $s_l < s_a < s_h$ we replace $\mathbf{y}_l$ by $\mathbf{y}_a$. Otherwise, we go to step 5b.

b) **Expansion or contraction**.

1) **Expansion**: If $s_a > s_h$ (i.e., we have a new maximum) we expand $\mathbf{y}_a$ to $\mathbf{y}_b$ as follows:

$$\mathbf{y}_b = \gamma\mathbf{y}_a + (1-\gamma)\bar{\mathbf{y}},$$

where $\gamma > 1$ is another constant called *expansion coefficient*, which represents the ratio between the distances $[\mathbf{y}_b\bar{\mathbf{y}}]$ and $[\mathbf{y}_a\bar{\mathbf{y}}]$.
Then generate ${\mathbf{I}_\mathbf{R}}^b$ and compute $s_b = \mathcal{V}(\mathbf{T}, {\mathbf{I}_\mathbf{R}}^b)$. If $s_b > s_h$, we replace $\mathbf{y}_l$ by $\mathbf{y}_b$. Otherwise, we have a failed expansion and replace $\mathbf{y}_l$ by $\mathbf{y}_a$.

2) **Contraction**: If we have reached this step, then $s_a \leq s_l$ (i.e. replacing $\mathbf{y}_l$ by $\mathbf{y}_a$ would leave s_a as the new minimum). Afterwards we compute

$$\mathbf{y}_b = \beta\mathbf{y}_l + (1-\beta)\bar{\mathbf{y}},$$

where $0 < \beta < 1$ is the *contraction coefficient*, defined as the ratio between the distances $[\mathbf{y}_b\bar{\mathbf{y}}]$ and $[\mathbf{y}_l\bar{\mathbf{y}}]$.
Then generate ${\mathbf{I}_\mathbf{R}}^b$ and compute $s_b = \mathcal{V}(\mathbf{T}, {\mathbf{I}_\mathbf{R}}^b)$. If $s_b > \max(s_l, s_a)$, then we replace $\mathbf{y}_l$ by $\mathbf{y}_b$; otherwise, the contracted point is worse than $\mathbf{y}_l$, and for such a failed contraction we replace all the $\mathbf{y}_i$'s by $(\mathbf{y}_i + \mathbf{y}_h)/2$.

6. With the new $\mathbf{y}_l$ value, update the simplex and return to step 4.

Stopping criteria. The hill climbing algorithm stops when $s_h \geq \delta$ (i.e., the image has been successfully reconstructed) or when the maximum number of iterations is reached (i.e., the reconstruction has failed).

Rationale behind the algorithm. As stated in [Mathews and Fink, 2004], when we move from the worst vertex ($\mathbf{y}_l$) towards any of the other vertices, the function value s increases. Hence, assuming a continuous fitness function $\mathcal{V}$ with a relatively smooth surface following a general commanding gradient (which is the usual case for unprotected biometric systems), it is feasible that a point $\mathbf{y}_a$ lying on the line $[\bar{\mathbf{y}}\mathbf{y}_l]$ on the opposite side of $\mathbf{y}_l$ with respect to the hyperplane defined by the other k points (i.e., outside the simplex) achieves higher values of

$\mathcal{V}$. If the function value s_a is higher than the value of all vertices, then we have most likely moved in the correct direction, and the maximum may lie ahead. This is the case in step 5.b.1, when the point is further expanded in the same direction. On the other hand, if the new point $\mathbf{y}_a$ results in a new minimum (i.e., its function value s_a is lower than in any other vertex), the maximum is probably close to $\mathbf{y}_l$. Therefore, the simplex is contracted by finding a new point in the $[\mathbf{y}_l\bar{\mathbf{y}}]$ line inside rather than outside the simplex, as in case 5.b.2. If this new point achieves no improvement over $\mathbf{y}_l$, the only remaining option is contracting the whole simplex: the maximum probably lies inside the simplex. For clarity, all these scenarios are depicted in Fig. 4.3 for the two dimensional case, where the simplex is a triangle.

Additional note. It has to be emphasized that the Uphill Simplex is not used to optimize the templates $\mathbf{T}$ deployed by the development recognition system, but the vectors $\mathbf{y}$ needed by the hand shape generator (which do not coincide with $\mathbf{T}$, see Eq. 4.1). This way, the proposed approach is general as it can be used to reconstruct the handshape images independently of the template $\mathbf{T}$ (e.g., size, format, information stored, ...) used by the system. Furthermore, due to the random initialization of the optimization algorithm (step 2), different synthetic samples can be reconstructed from a single template.

Lastly, it should be born in mind that a development pool of subjects is necessary to determine the initialization parameters of the hand shape generator and the Uphill Simplex, namely: *i*) the dimensionality (k) of the vector $\mathbf{y}$, *ii*) the PCA matrix P, *iii*) the mean $\bar{x}$ of the development set of hand shape images, and *iv*) the statistical model G for the Uphill Simplex.

4.1.2. Attacking Iris Binary Templates: Inverse Biometrics Based on a Genetic Algorithm

In the context of iris-based recognition systems, the problem stated in Sect. 4.1 can be solved using a probabilistic approach based on a real-valued genetic algorithm. As mentioned in Chapter 2, in the context of iris recognition a very recent study has been the first to address the problem of generating iris images from binary iriscodes [Venugopalan and Savvides, 2011]. In that work, the authors take advantage of the prior knowledge of the feature extraction scheme used by the recognition system (i.e., functions defining the filters used during feature extraction) in order to reverse engineer the iriscode. Then, real images are used to impart a more realistic appearance to the synthetic iris patterns generated.

The differences between the deterministic technique described in [Venugopalan and Savvides, 2011] and the probabilistic method proposed in this Dissertation will be pointed out throughout the section. However, the most important differences are as follows:

- **Type of approach**. In [Venugopalan and Savvides, 2011], given an iriscode and a fixed set of parameter values, the resulting reconstructed synthetic pattern is always the same (i.e., deterministic approach). Our methodology allows the reconstruction of potentially a large number of synthetic iris patterns with very similar iriscodes (i.e., probabilistic approach). As will be shown in the experimental analysis (Sect. 4.2.2), having more than

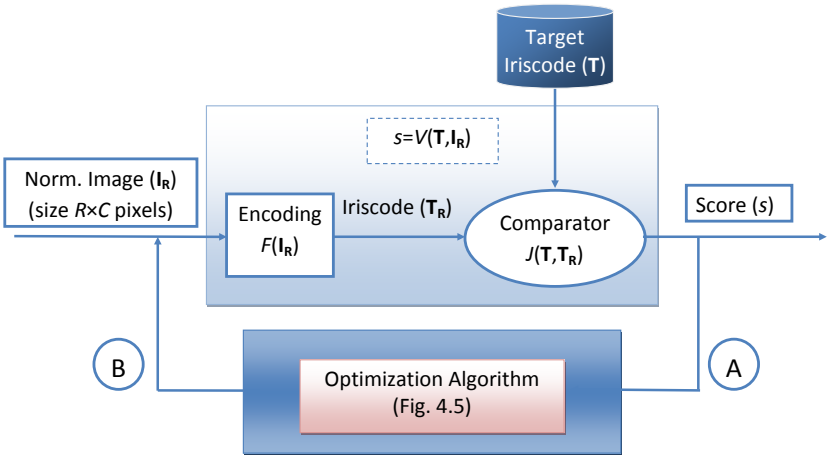


Figure 4.4: General diagram of the binary templates reconstruction method. *A detailed diagram of the reconstruction approach (dashed rectangle) is given in Fig. 4.5, where points A and B show, respectively, the input and output of the algorithm.*

one synthetic iris significantly increases the chances of a positive match to the genuine samples.

- **Knowledge required**. The method proposed in [Venugopalan and Savvides, 2011] requires knowledge of the feature extraction scheme being used by the recognition system. On the contrary, our technique only requires the output score of an iris matcher to reconstruct the image and does not need any prior information about how the recognition system obtains that score.

- **Images required**. In order to generate somewhat realistic iris-like patterns, the algorithm described in [Venugopalan and Savvides, 2011] relies on information from real iris images. No real iris images are needed in the present study to obtain realistic-looking synthetic images.

- **Experimental protocol**. Although consistent, the experimental protocol followed in [Venugopalan and Savvides, 2011] does not allow for the comparison of its results with other methods, as the iris matchers used for development and validation are proprietary implementations and not publicly available. In the present chapter, the experimental protocol has been designed to be fully reproducible so that an objective comparison may be carried out with other reconstruction approaches proposed in the future.

Taking those considerations into account, the problem stated in Sect. 4.1 may be solved using a genetic algorithm to optimize the similarity score given by the system, according to the general diagram shown in Fig. 4.4. Genetic algorithms, which have shown remarkable performance in optimization problems [Goldberg, 1989], are randomized hill-climbing beam search methods that iteratively apply certain rules inspired by biological evolution to a population of individuals (possible solutions) according to a given fitness function. During each iteration the algorithm

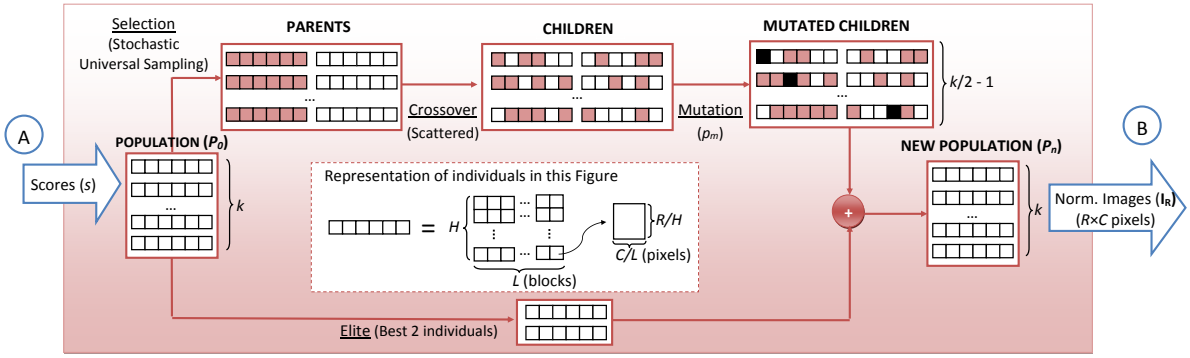


Figure 4.5: Diagram of the probabilistic method *proposed in the present chapter for the reconstruction of iris images from their iriscode. Points A and B (input and output of the optimization algorithm respectively) may be seen for reference in Fig. 4.4. As is shown in the shaded chart in the center of the figure, although individuals are represented as vectors for simplicity, strictly they are matrices of size $R \times C$ pixels divided into $H \times L$ blocks.*

moves towards better solutions in terms of the fitness function which has to be optimized. In our particular problem, the following observations ought to be made.

- The fitness value associated with each individual (normalized iris image) is the matching score, $s = \mathcal{V}(\mathbf{T}, \mathbf{I_R})$.
- Usually genetic algorithms operate with individuals that are binary vectors. In this problem, the genetic algorithm has been modified to work with matrices of real values (i.e., $\mathbf{I_R}$) where each of the $H \times L$ blocks represents a gene of the individual.
- Consider a $R \times C$ dimensional matrix $\mathbf{I_R}$ of real values, which is divided into $H \times L$ square blocks of dimension $R/H \times C/L$, with $H \leq R$ and $L \leq C$. This matrix is mapped by some unknown function $\mathcal{F}$ to a binary matrix $\mathbf{T_R}$ (i.e., $\mathbf{T_R} = \mathcal{F}(\mathbf{I_R})$) of dimensions $K \times W$ (K is a multiple of R and W is a multiple of C).

Keeping those observations in mind, the steps followed by the reconstruction algorithm are (see Fig. 4.5):

1. Generate an initial population P_0 with k individuals of size $R \times C$ (i.e., dimensions of the normalized iris images), and tessellate each individual into $H \times L$ rectangular blocks.
2. Compute the similarity scores s^i of the individuals ($\mathbf{I_R}^i$) of the population P_0, $s^i = \mathcal{V}(\mathbf{T}, \mathbf{I_R}^i)$, with $i = 1, \ldots, N$.
3. Four rules are used at each iteration to create the next generation P_n of individuals from the current population:

   a) **Elite**: The two individuals with the maximum similarity scores are retained unaltered for the next generation.

b) **Selection**: Certain individuals, the *parents*, are chosen by stochastic universal sampling [Baker, 1987]. Therefore, the individuals with the highest fitness values (similarity scores) are more likely to be selected as parents for the next generation: one subject can be selected 0 or many times. From the original N individuals, only $N-2$ are eligible (as the best two are retained as elite) from which $N/2-1$ *fathers* and $N/2-1$ *mothers* are chosen.

c) **Crossover**: Parents are combined to form $N-2$ *children* for the next generation by employing a scattered crossover method: a random binary matrix of size $H \times L$ is created and the genes (blocks) for the first child are selected from the first parent if the value of an entry is 1, and from the second when it is 0 (vice-versa for the second child).

d) **Mutation**: Random changes are applied to the blocks of the new children with a mutation probability p_m. When a certain block is selected for mutation, the equivalent block in the individual of the population with the highest fitness value is changed.

4. Redefine $P_0 = P_n$ and return to step 2.

Stopping criteria. The algorithm stops when: *i*) the best fitness score of the individuals in the population is higher than the threshold δ (i.e., the image has been successfully reconstructed), *ii*) the variation of the similarity scores obtained in successive generations is lower than a previously fixed value, or *iii*) when the maximum number of generations (iterations) is exceeded.

Rationale behind the algorithm. A genetic search algorithm was used in this section, since the nature of the search space is unknown to us. Specifically, it is not clear if the objective function results in a smooth or even a continuous search space. Consequently, classical stochastic gradient descent methods could not be used. Although the previous work in [Rathgeb and Uhl, 2010b] partially supports the assumption of smoothness/continuity, this could not be easily substantiated in our case. Therefore, by simultaneously searching for multiple solutions in the solution space, genetic algorithms are more likely to avoid potential minima or even plateaus in the search space (much like simulated annealing schemes).

Additional note. In addition to the important characteristics of the reconstruction method presented at the beginning of this section, which differentiate it from other previously published iris reconstruction techniques [Venugopalan and Savvides, 2011], one more fact should be highlighted: no *real* iris images are involved in the reconstruction process. As will be explained in Sect. 4.2.2, the initial population P_0 is taken from a database of fully *synthetic* iris images.

4.2. Experimental Evaluation

In this experimental section, we will use the algorithms proposed in Sect. 4.1 to analyse the irreversibility of unprotected templates, as part of the security and privacy evaluation methodology defined in Chapter 3. To that end, the experimental framework has been designed not

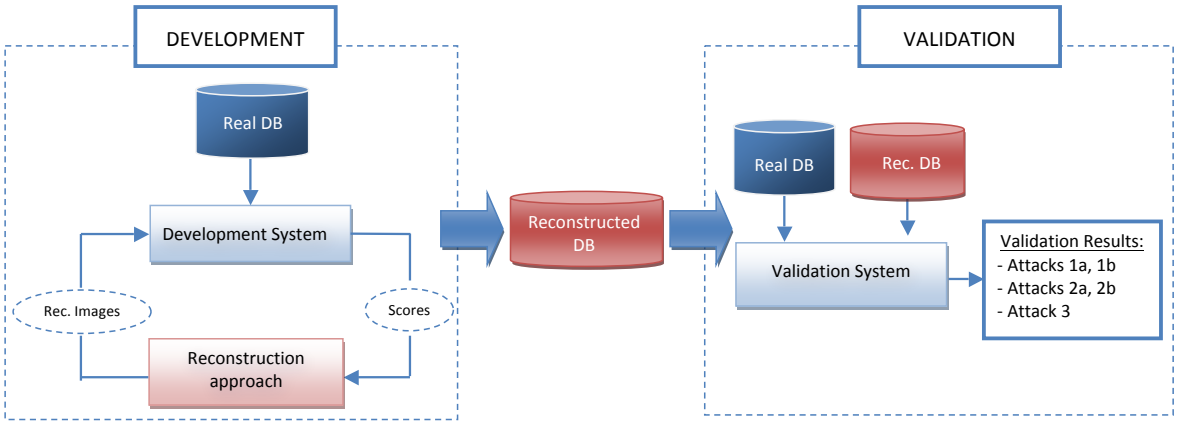


Figure 4.6: *Two-stage experimental protocol followed in the experimental evaluation: i) in the development stage, the reconstructed database is generated, and ii) in the validation stage, the privacy threat posed by the reconstructed samples is evaluated launching attacks. In order to obtain unbiased results, different biometric systems are used at each stage (i.e., development and validation). Finally, real databases are depicted in blue, and synthetic databases in red.*

only to avoid biased results, but also to estimate the degree of compliance of the proposed reconstruction approaches with the next main objectives:

- Determine the feasibility of recovering a biometric sample from its template.
- Evaluate to what extent the reconstructed samples are able to compromise the security and privacy granted by biometric recognition systems.
- Determine whether it is possible to generate different synthetic reconstructed samples from one given template.

Keeping those goals in mind, a two-step protocol is proposed, divided into a development and a validation stage, as depicted in Fig. 4.6:

- **Development**. The purpose of this stage is twofold: *i*) on the one hand, train any module if necessary; *ii*) on the other hand, generate the synthetically reconstructed datasets that will be used in the validation stage.
- **Validation**. The objective of this stage is to validate the proposed reconstruction scheme and to estimate its performance. For this purpose, the synthetically reconstructed samples generated in the development stage are presented to a different biometric system to determine if they are positively matched to the genuine original images, which would mean that the reconstruction approach is successful and, as a consequence, templates are reversible. In particular, three different types of attacks are carried out, reporting the Success Rates (SR) for each case, as defined in Sect. 3.2. If the reported SRs are high, we can conclude that traditional or unprotected biometric systems do not grant the necessary privacy to the subjects.

The key factors to compute the SR are to define: *i*) what constitutes an attack, and *ii*) when an attack is considered to be successful. For the present analysis of the unprotected templates irreversibility, three representative attacks will be taken into account in order to estimate the performance of the proposed reconstruction methods:

1. **Attack 1**: 1 reconstructed image *vs* 1 real image. In this case the attack is carried out on a 1-on-1 basis. That is, one reconstructed image is compared to one real image and, if the resulting score exceeds the fixed verification threshold, the attack is deemed to be successful. Two possible scenarios may be distinguished in this case, depending on the real image being attacked:

   a) **Attack 1a**. The real image being attacked is the original sample from which the synthetic image was reconstructed.

   b) **Attack 1b**. The real image being attacked is one of the other samples of the same subject present in the real database.

2. **Attack 2**: N reconstructed images *vs* 1 real image. In this case all N reconstructed images are compared to the real sample. The attack is successful if at least one of the synthetic images positively matches the real template. This represents the most likely attack scenario analysed in other related vulnerability studies [Cappelli *et al.*, 2007], where the template of a legitimate subject in the database is compromised and the intruder reconstructs multiple images to try and break the system. The attacker will gain access if any one of the reconstructed images results in a positive score.

   The same two scenarios as in attack 1 can be considered here:

   a) **Attack 2a**. The real image being attacked is the original sample from which the synthetic images were reconstructed.

   b) **Attack 2b**. The real image being attacked is one of the other samples of the same subject present in the real database.

3. **Attack 3**: N reconstructed images *vs* average (M real images). It is a common practice in many biometric recognition systems to compare the probe sample to several stored templates and return the average score. To emulate this scenario, each reconstructed image is compared to the M samples of the real subject available in the database. The attack is successful if the average score due to the comparison of *any of the N reconstructed images* is higher than the given verification threshold.

For the development and validation stages, different unprotected systems and databases (described respectively in Sects. 3.3 and 3.4) have been used in order to avoid biased results. All of them are either publicly available, commercial or well described in the literature so that the experiments are fully reproducible and the results here presented may be compared with future similar works.

Two additional facts should be also noted: *i*) while the real databases used for the experiments are depicted in blue in Fig. 4.6, synthetic databases are highlighted in red, and *ii*) several systems will be tested on the validation experiments (see Figs. 4.7 and 4.10 for more details on the databases and systems used in each case study).

4.2.1. Irreversibility Evaluation of Handshape-Based Verification Systems

As mentioned in Sect. 4.1.1, and depicted in Fig. 4.7, before reconstructing the images, we need to complete the training of the hand synthesizer and fix the initialization parameters (k, P, G and $\bar{x}$) of the reconstruction algorithm. As a consequence, three different databases are used in the experiments:

- First, images from the GPDS2 DB [Morales *et al.*, 2012], described in Sect. 3.4.1.2, are used for training.

Once the hand shape generator has been trained, it is combined with the Uphill Simplex algorithm as described in Sect. 4.1.1 to reconstruct the hand images from two real databases, acquired with different devices and conditions:

- The GPDS DB [Ferrer *et al.*, 2007], described in Sect. 3.4.1.1.
- The UST DB [The Hong Kong University of Science and Technology, Department of Computer Science], described in Sect. 3.4.1.2.

This leads to the generation of two synthetic databases: S-GPDS DB and S-UST DB, respectively.

It is important to notice that, while the images used to train the hand generator and to compute the initialization parameters are taken from the GPDS2 database [Morales *et al.*, 2012], the real hand shape samples to be reconstructed are taken from the GPDS [Ferrer *et al.*, 2007] and the UST [The Hong Kong University of Science and Technology, Department of Computer Science] databases. As a consequence, the images used to train the generator are independent and belong to completely different subjects than those being reconstructed, hence preventing optimistically biased validation results.

Additionally, the capturing devices used in the acquisition of the two real databases to be reconstructed are completely different: the GPDS DB was captured using a digital scanner and the UST DB using a CCD camera. Thus, while hands are placed on a glass platen in the first case, leading to a certain distortion on the acquired image, hands belonging to the UST DB are captured using a contactless protocol so that no distortion is produced. This way we will be able to determine to what extent the proposed reconstruction approach is able to generate samples acquired under totally different conditions.

Regarding the unprotected systems used, in the development step, a single system is used to reconstruct the hand images:

- Development geometry-based system [Ferrer and Morales, 2011], described in Sect. 3.3.1.1.

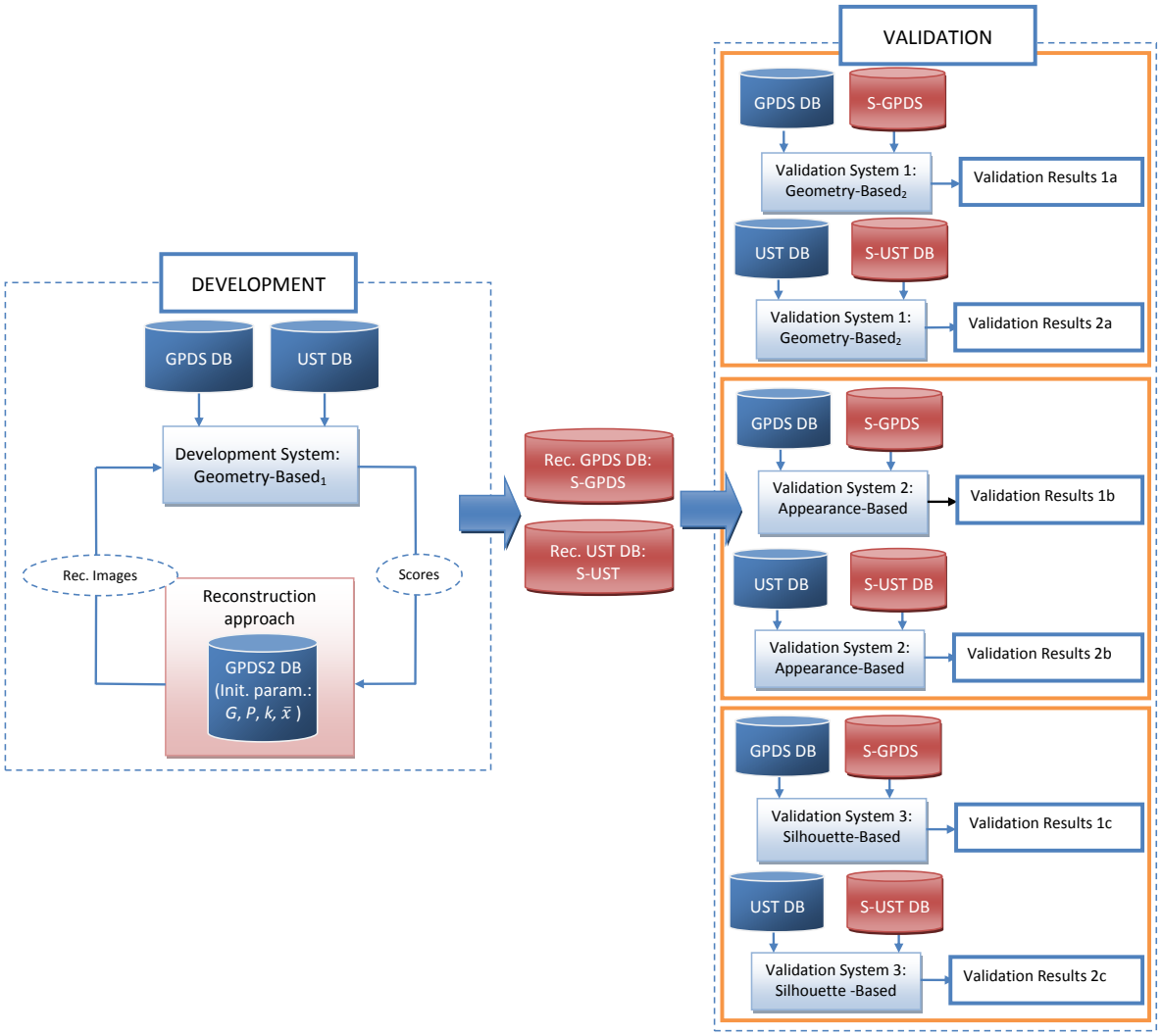


Figure 4.7: *Two-stage experimental protocol followed in the hand-based verification evaluation: i) in the development stage, the initialization parameters (G, P, k, $\hat{x}$) are trained on the real GPDS2 DB, and two reconstructed databases are generated (S-GPDS and S-UST), and ii) in the validation stage, the privacy threat posed by the reconstructed samples is evaluated on three different systems (geometry-, appearance- and silhouette-based). Real databases are depicted in blue, and synthetic databases in red.*

On the other hand, in the validation step three systems based in different sets of features are used to test whether the images obtained in the previous stage are positively matched to real samples of the genuine subject by completely independent systems. In particular, the following systems are evaluated:

- Validation geometry-based [Burgues *et al.*, 2009], described in Sect 3.3.1.2.
- Validation appearance-based [Yörük *et al.*, 2006], described in Sect. 3.3.1.3.
- Validation silhouette-based features [Ferrer and Morales, 2011], described in Sect. 3.3.1.3.

4.2.1.1. Development Experiments: Reconstructing Images

Exhaustive development experiments were carried out on the GPDS2 DB to determine the four initialization parameters of the hand shape generator [Cootes *et al.*, 2001, 1995], namely: *i*) the dimensionality (k) of the vector $\mathbf{y}$, which was finally set to $k = 50$ dimensions, thus taking into account 99.9% of the variance in the trained model; *ii*) the PCA matrix P; *iii*) the statistical model G, which was defined as a uniform distribution within the limits $[-3\sqrt{\lambda_j}, 3\sqrt{\lambda_j}]$, being λ_j the eigenvalue corresponding to the j-th eigenvector of matrix P (with $j = 1, \ldots, k$); and *iv*) the mean $\bar{x}$ of the development set of hand shape images.

In our previous work [Gomez-Barrero *et al.*, 2011], we carried out an exhaustive set of experiments in order to select the best possible values for the parameters of the Uphill Simplex (α, β and γ). Since the goal of the Dissertation is not finding the optimal parameter set, but proving the efficiency and feasibility of the proposed reconstruction method as well as providing an estimation of the hand recognition systems vulnerabilities to the reconstruction scheme, no further experiments have been run to determine new values for these parameters. Furthermore, by using the same values, we are also testing the robustness of the Uphill Simplex algorithm against different biometric characteristics.

More specifically, we performed three successive steps fixing in each of them two of the parameters and sweeping the other in a given range. According to the original Downhill Simplex algorithm [Nelder and Mead, 1965], the best values for the parameters are $\alpha = 1$, $\gamma = 2$ and $\beta = 0.5$. Thus, the selected ranges were centred on those values, taking always into account the constraints explained in Sect. 4.1.1, namely: $\alpha > 0$, $\gamma > 1$ and $0 < \beta < 1$. Finally, the parameters values were set to $[\alpha, \gamma, \beta] = [1.1, 1.1, 0.8]$.

In order to determine the positive matching threshold δ at which a hand shape sample is considered to have been successfully reconstructed, the geometry-based recognition system accuracy was analysed on the GPDS DB. Each of the 144 subjects comprised in the database was modelled with four samples randomly selected from the ten samples available, and the matching process was repeated five times training the subject models with four different samples (random selection) each time. In each of the five iterations of this process, mated scores were computed matching the remaining six samples with the subject model (i.e., $144 \times 6 \times 5 = 4,320$ mated scores), while non-mated scores were generated comparing these same six samples of each subject

Table 4.1: *Reconstruction rate and average number of comparisons needed to reconstruct a hand (in brackets) for the two databases reconstructed in the experiments (GPDS DB and UST DB). Results are given for the reconstruction method proposed in the Dissertation and for an eventual brute force reconstruction (as baseline).*

	GPDS DB	UST DB
Rec. Method	100% (109)	100% (215)
Brute Force	52% (15,746)	31% (17,562)

to the remaining subjects' models (i.e., $144 \times 143 \times 6 \times 5 = 617,760$ non-mated scores). The threshold δ was finally fixed at the operating point corresponding to FMR = 0.01%, since the probability of having a non-mated score at that point is very low: only one impostor in 10,000 would access the system. Thus, two hand shape images producing a similarity score greater than δ may be considered to belong to the same subject.

After the initialization parameters were fixed, we reconstructed the hand shapes contained in the two real validation databases: GPDS DB and UST DB. Each subject was modelled in the development system with just one randomly selected hand image, and three synthetic samples were generated using the reconstruction method proposed. Those synthetic samples constitute the synthetic validation databases: S-GPDS DB and S-UST DB.

For completeness and also as baseline result with which to compare the performance of our reconstruction method, a brute force reconstruction approach (i.e., an exhaustive search through a very large number of hand shape images) was also carried out. For this purpose, 20,000 synthetic hand shapes were randomly generated with the hand generator (${\mathbf{I_R}}^m$ with $m = 1, \ldots, 20,000$). As the development system is working at an operating point where, on average, one *real* hand image in 10,000 would produce a false positive, it seems that 20,000 may be a reasonable number of *synthetic* samples to find one that is assigned to a given real identity. Therefore, those images were matched to the subjects of each database (GPDS DB and UST DB) until one of the synthetic samples produced a score greater than δ. The number of comparisons needed by the brute force strategy to reconstruct a given hand is M, being ${\mathbf{I_R}}^M$ the first image that produced the winning score.

The results of both reconstruction approaches (the one proposed in the present chapter and the brute force method) are shown in Table 4.1, in terms of the reconstruction rate (i.e., percentage of successfully reconstructed hands) and the average number of comparisons necessary to reconstruct a hand image. We can observe that only around 40% of the hand shapes were recovered by the brute force scheme, while all of them were successfully reconstructed using the method proposed in the present chapter. Furthermore, the Uphill Simplex-based method is over 100 times faster than the brute force strategy. Therefore, not only the hand shapes are reconstructed with a considerably lower number of comparisons by the Uphill Simplex-based approach, but it also guarantees success in the reconstruction, in contrast to the brute force

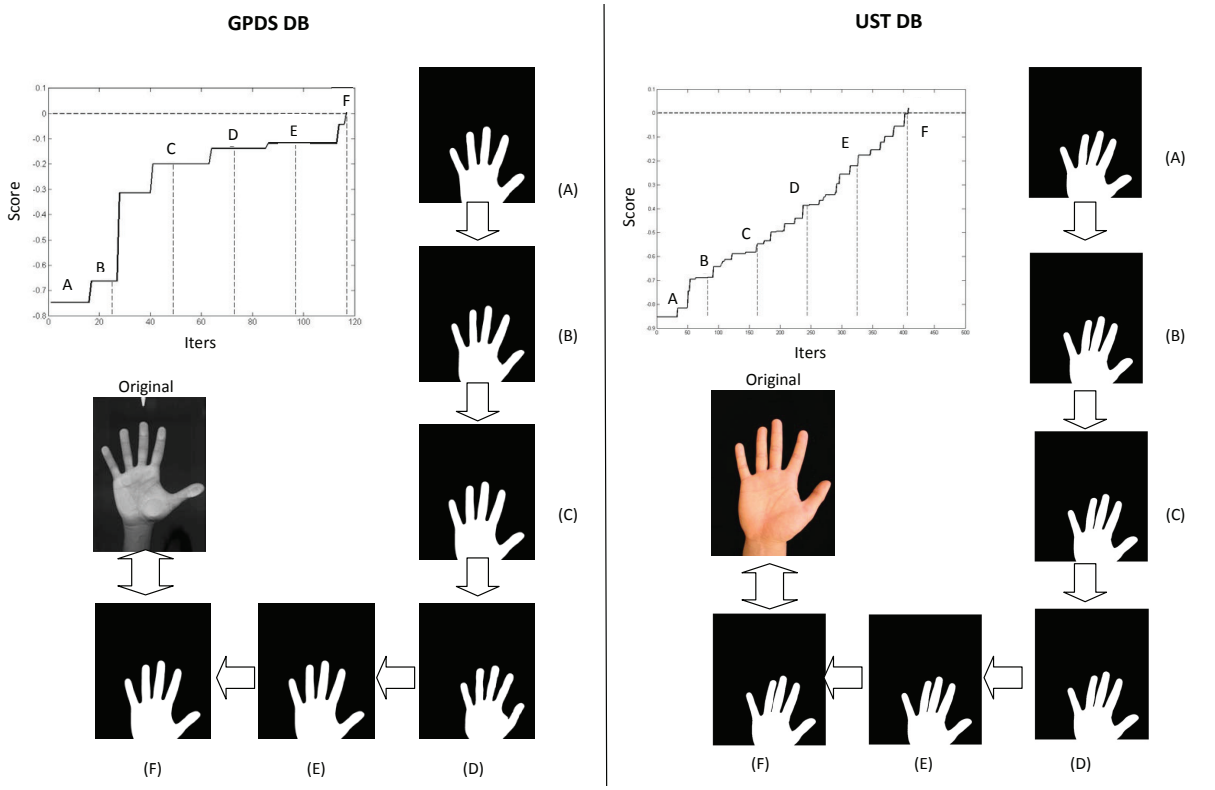


Figure 4.8: *Examples of the evolution of the score and the synthetic hand shapes through the iterations of the proposed algorithm for a successfully reconstructed hand shape of the GPDS DB (left) and of the UST DB (right). The horizontal dashed line represents the objective threshold (δ) where a sample is considered to have been successfully reconstructed.*

scheme.

Finally, in Fig. 4.8 the evolution of the hand shapes ($\mathbf{I_R}$) through the iterative reconstruction process for one subject of each validation database is depicted. The score evolution is also shown, where the horizontal dashed line represents the objective threshold (δ). Starting from a random hand (iteration A), it can be seen that the successive synthetically generated samples evolve towards the original hand (iterations B-E), until the score given by the development recognition system is higher than δ: the hand image has been successfully reconstructed (iteration F).

4.2.1.2. Validation Experiments: Attacking Unprotected Systems

As explained at the beginning of the present section, the reconstructed images (S-GPDS DB and S-UST DB) are used to try to access (i.e., attack) the validation systems, thereby evaluating the security and privacy threat they pose. Since several systems are used in this validation step, and the appearance- and silhouette-based systems work on independent features with respect to the ones used by the development system (geometry-based), the results obtained in this validation stage for each database permit to evaluate in an objective way the ability of the proposed reconstruction approach to recover the handshape images from their templates.

Table 4.2: *Total number of attacks carried out for each experiment and each handshape database.*

	GPDS DB	UST DB
A_{T1a}	$144 \times 3 = 432$	$564 \times 3 = 1,692$
A_{T1b}	$144 \times 3 \times 9 = 3,888$	$564 \times 3 \times 9 = 15,228$
A_{T2a}	144	564
A_{T2b}	$144 \times 9 = 1,296$	$564 \times 9 = 5,076$
A_{T3}	144	564

The performance of the attacks is measured in terms of its Success Rate (SR), which is defined as the expected probability of bypassing the attacked system (see Sect. 3.2). Table 4.2 shows a summary of the total number of attacks carried out for each experiment and database, where sub-indices denote the attack under consideration. Furthermore, SR will be computed at three operating points corresponding to: FMR = 0.1%, FMR = 0.05%, and FMR = 0.01%, which, according to [ANSI/NIST, 2009], correspond to a low, medium and high security application, respectively. For completeness, the system is also tested at a very high security operating point corresponding to FMR $\ll$ 0.01%. Depending on the experiment at hand, these operating points are estimated (on the GPDS DB or the UST DB), considering subject models computed with either one hand image (for attacks 1 and 2) or four hand images (attack 3) for each of the validation systems tested.

Several observations can be made from the results of the validation experiments shown in Tables 4.3 to 4.8:

- The high performance of the reconstruction algorithm is confirmed. As expected, the performance of the synthetic images is higher when a system based on the same kind of features as the ones used in the development stage (hand geometry) is used. However, the SR for the other validation systems, based on completely independent sets of features, remains considerably high:
  - In the case of the geometry-based recognition system, the SR reaches an average SR of over 85% for the three usual operating points considered and over 90% for the most likely attacking scenario for the UST DB (i.e., SR_{2a}).
  - For the other two validation systems (appearance- and alignment-based), the SR remains between 50 and 60% on average for the three usual operating points considered.
- Even for an unrealistically high security point (i.e., FMR $\ll$ 0.01%), the reconstructed images would have, on average,
  - Around 80% chances of entering the geometry-based system for both databases tested.
  - Between 30 and 45% chances of breaking the system for the GPDS DB and over 35% for the UST DB under the appearance- and silhouette-based systems.

Table 4.3: *SR of the different attacking scenarios considered against the* ***geometry-based system*** *using the GPDS DB at the four operating points tested.*

FMR	GPDS DB - Geometry-based system					
	SR_{1a}	SR_{1b}	SR_{2a}	SR_{2b}	SR_3	**Average**
0.1%	90.26	87.52	90.26	87.52	92.58	89.63
0.05%	88.96	85.89	88.96	85.89	90.61	88.06
0.01%	85.41	83.27	85.41	83.27	87.37	84.95
$\ll$0.01%	78.97	75.96	78.97	75.96	81.05	78.20

Table 4.4: *SR of the different attacking scenarios considered against the* ***appearance-based system*** *using the GPDS DB at the four operating points tested.*

FMR	GPDS DB - Appearance-based system					
	SR_{1a}	SR_{1b}	SR_{2a}	SR_{2b}	SR_3	**Average**
0.1%	58.82	53.38	58.82	53.38	60.78	57.04
0.05%	52.94	41.39	52.94	41.39	58.82	49.50
0.01%	50.98	36.60	50.98	36.60	54.90	46.01
$\ll$0.01%	31.37	23.97	31.37	23.97	43.14	30.76

Table 4.5: *SR of the different attacking scenarios considered against the* ***silhouette-based system*** *using the GPDS DB at the four operating points tested.*

FMR	GPDS DB - Silhouette-based system					
	SR_{1a}	SR_{1b}	SR_{2a}	SR_{2b}	SR_3	**Average**
0.1%	62.52	61.28	62.52	61.28	65.27	62.57
0.05%	60.26	51.02	60.26	51.02	63.57	57.23
0.01%	58.92	40.65	58.92	40.65	61.49	52.13
$\ll$0.01%	45.25	34.97	45.25	34.97	55.66	43.22

Table 4.6: *SR of the different attacking scenarios considered against the* ***geometry-based*** *system using the UST DB at the four operating points tested.*

FMR	UST DB - Geometry-based system					
	SR_{1a}	SR_{1b}	SR_{2a}	SR_{2b}	SR_3	**Average**
0.1%	93.29	90.59	93.29	90.59	95.68	92.69
0.05%	92.58	88.95	92.58	88.95	94.56	91.52
0.01%	90.15	86.21	90.15	86.21	92.98	89.14
$\ll$0.01%	80.27	78.51	80.27	78.51	85.24	80.56

Table 4.7: *SR of the different attacking scenarios considered against the* ***appearance-based system*** *using the UST DB at the four operating points tested.*

FMR	UST DB - Appearance-based system					
	SR_{1a}	SR_{1b}	SR_{2a}	SR_{2b}	SR_3	**Average**
0.1%	63.58	57.97	63.58	57.97	66.21	61.86
0.05%	57.25	43.46	57.25	43.46	63.25	52.93
0.01%	54.69	40.65	54.69	40.65	59.82	50.10
$\ll$0.01%	38.25	29.52	38.25	29.52	51.29	37.37

Table 4.8: *SR of the different attacking scenarios considered against the* ***silhouette-based system*** *using the UST DB at the four operating points tested.*

FMR	UST DB - Silhouette-based system					
	SR_{1a}	SR_{1b}	SR_{2a}	SR_{2b}	SR_3	**Average**
0.1%	52.36	50.28	52.36	50.28	53.24	51.70
0.05%	50.53	47.52	50.53	47.52	51.98	49.62
0.01%	48.27	44.59	48.27	44.59	50.37	47.22
$\ll$0.01%	35.67	33.28	35.67	33.28	45.29	36.64

- The results are very similar for the appearance- and silhouette-based systems. The only significant difference is the decrease of the SR for the latter when working on the UST DB. The reason behind this worsening is a decrease in the accuracy of the system: silhouette alignment is not as competitive as in the case of the GPDS DB due to projection distortions caused by the camera acquisition scenario, which leads to a higher EER. Thus, for identical FMR operating points, the FNMR is higher and therefore more hand images within the intra-subject variability are rejected.

- The probabilities of accessing the system in the scenarios 1.a and 2.a, 1.b and 2.b are the same for each validation system considered. This means that the validation system is quite robust to several initializations of the Uphill Simplex algorithm (i.e., reconstructions of the same template). This way, the scores given by the system do not vary significantly among reconstructions, which means that either all three or none of them are able to access the system.

- As expected, it is more probable that the synthetic samples are positively matched to the original image from which they were reconstructed than to other real images of the same subject (see the decrease in the SR between SR_{1a} *vs* SR_{1b} and between SR_{2a} *vs* SR_{2b}).

- Even so, the reconstructed images still present a high probability of breaking the system even when the stored templates are not the one from which they were recovered (average SR of SR_{1b} and SR_{2b} around 45% for the appearance- and silhouette-based systems).

- Furthermore, for the case of using several real samples of the subject for verification (SR_3), the reconstructed samples are still able to access the system for:

  - Around 92% of the attempts in the usual operating points, and for almost 80% in the extremely high operating point tested for the geometry-based validation system.
  - Around 60% of the attempts in the usual operating points, and for almost 50% in the extremely high operating point tested for the remaining two validation systems.

The results presented in Tables 4.3 to 4.8 confirm the first and second objectives set in the present chapter: hand shape images may be recovered from their templates, and the reconstructed images represent a real threat to the integrity of automatic recognition systems. In other words, unprotected templates are reversible, hence putting the privacy of the subject at risk.

Recall now that the third goal of the chapter is to determine the feasibility of generating multiple synthetic hand images that yield templates very similar to a real one. In order to address this point, results from experiment 2.a (i.e., all 3 synthetic images are compared to the original from which they were reconstructed) are presented in Tables 4.9 to 4.11 from a different perspective. In this case we present in each column the percentage of attacks in which only n out of the 3 reconstructed images (with $n = 1, 2, 3$) were positively matched to their original real

Table 4.9: *Percentage of successful attacks where n out of the total three reconstructions were positively matched against the original hand image from which they were reconstructed. Results are given for the four operating points tested on the* ***geometry-based recognition system****.*

FMR	GPDS DB			UST DB		
	$n=1$	$n=2$	$n=3$	$n=1$	$n=2$	$n=3$
0.1%	0	0	90.26	0	0	93.29
0.01%	0	0	88.96	0	0	92.58
0.05%	0	0	85.41	0	0	90.15
$\ll$0.01%	0	0	78.97	0	0	80.27
Average	0	0	85.9	0	0	89.1

Table 4.10: *Percentage of successful attacks where n out of the total three reconstructions were positively matched against the original hand image from which they were reconstructed. Results are given for the four operating points tested on the* ***appearance-based recognition system****.*

FMR	GPDS DB			UST DB		
	$n=1$	$n=2$	$n=3$	$n=1$	$n=2$	$n=3$
0.1%	0	0	58.82	0	0	63.58
0.01%	0	0	52.94	0	0	57.25
0.05%	0	0	50.98	0	0	54.69
$\ll$0.01%	0	0	31.37	0	0	38.25
Average	0	0	48.6	0	0	53.4

Table 4.11: *Percentage of successful attacks where n out of the total three reconstructions were positively matched against the original hand image from which they were reconstructed. Results are given for the four operating points tested on the* ***silhouette-based recognition system****.*

FMR	GPDS DB			UST DB		
	$n=1$	$n=2$	$n=3$	$n=1$	$n=2$	$n=3$
0.1%	0	0	62.52	0	0	52.36
0.01%	0	0	60.26	0	0	50.53
0.05%	0	0	58.92	0	0	48.27
$\ll$0.01%	0	0	45.25	0	0	35.67
Average	0	0	56.7	0	0	46.7

image. For all cases the total attacks performed is $A_{Tn} = 144$ for the GPDS DB and $A_{Tn} = 564$ for the UST DB, and the success rate will be noted as SR_n.

As it can be observed, for all the operating points tested, either all the synthetic samples ($n = 3$) or none of them were able to access the system: the columns $n = 1$ and $n = 2$ show a SR of 0% in all cases. This means that for all the subjects, it never occurred that only 1 or 2 of the reconstructions were positively matched to the subject model. However, averaging the four attacked operating points, all three reconstructions ($n = 3$) were positively matched to the original image for around 55% of the cases. These results confirm the third objective of the study: the ability of the proposed probabilistic reconstruction algorithm to generate multiple hand shapes that match one specific template.

But, why is this the case? Why do either all or none of the reconstructed images of one subject are able to access the system? A probable explanation to this fact is that, as previously explained in Sect. 4.2.1.1, the initialization parameters for both the Uphill Simplex (G distribution) and the hand shape generator (average hand $\bar{x}$ and PCA matrix P) remain constant across executions of the global algorithm: even though the G distribution is randomly sampled, the distribution does not change; and the same data is used to compute $\bar{x}$ and P. Therefore, the proposed method is able to reconstruct a hand sample as long as it lies within the variability range found in the development database: GPDS2 DB. This way, the reconstructed hand shapes deceive the system for a given subject either always ($n = 3$) or never ($n = 0$): in the first case, the subject samples fall within the development data variability range, while in the second case the subject discriminative characteristics are not modelled by the development dataset. Thus, in order to achieve a higher overall SR, the development database should be as big and statistically significant as possible.

It should also be noted that the experiments have also proven that the reconstruction method is robust to:

- Databases acquired under totally different conditions: in the GPDS DB a scanner where the hands were placed flat on the surface (thus leading to a certain degree of distortion in the images) was used, while the images of the UST DB were acquired with a CCD camera (no contact plastic distortion).

- Systems based on different sets of features: even though a geometry-based system was used in the development step, while in the validation stage experiments were carried out on systems based on geometric, general appearance- and silhouette-related features, the SR of the attacks was over 50% for the three realistic operating points tested.

Finally, in Fig. 4.9 some samples of both real and reconstructed hand images coming from the GPDS DB, S-GPDS DB, UST DB and S-UST DB are presented. As can be observed, the reconstructed hand shapes capture all the details of the original subject hands, such as the thick and short fingers of the fourth hand in the UST DB or the different curvatures of the outer part of the hand. Furthermore, we can also see that the three reconstructions of the same image vary

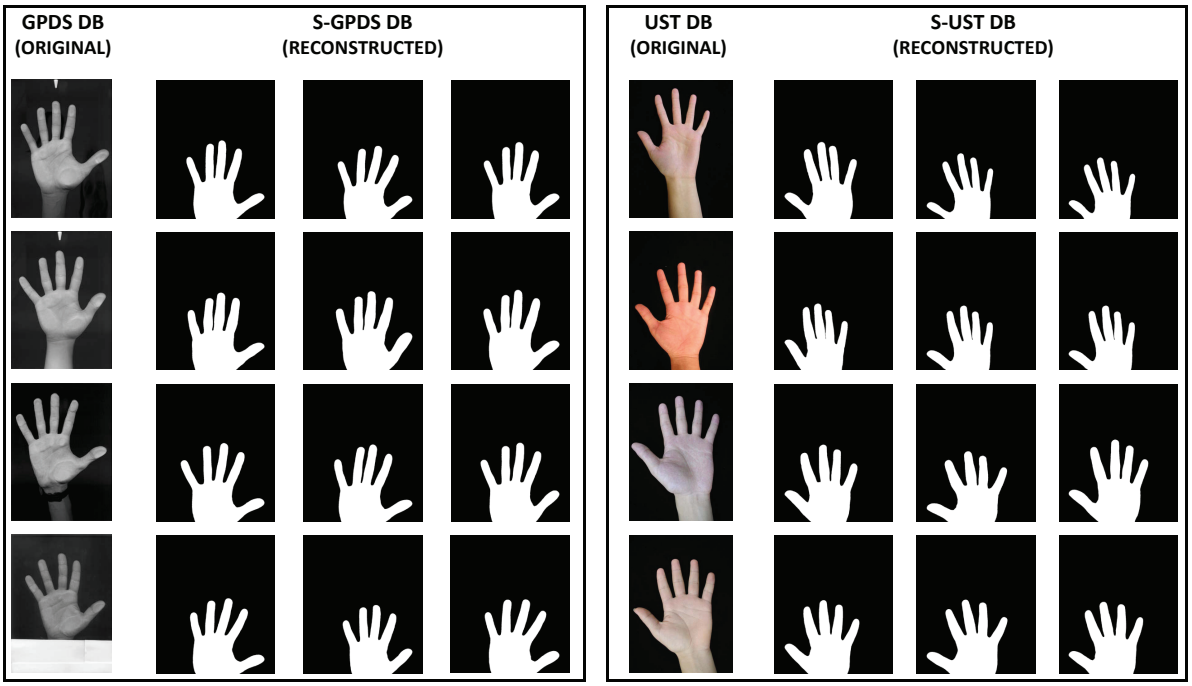


Figure 4.9: *Typical hand images that can be found in the real database (first column) with the three corresponding reconstructions (second to fourth columns) for the GPDS DB (left) and the UST DB (right).*

among themselves as could be expected from different real samples of the same subject (i.e., intra-subject variability): the position of the fingers is not the same in the three images and even the shape of the fingers is slightly different.

4.2.2. Irreversibility Evaluation of Iris-Based Verification Systems

In order to analyse the irreversibility of the binary iriscodes, we now use the inverse biometrics method described in Sect. 4.1.2, which needs a set of iris images for its initialization. This pool of initial samples is taken from a database of fully synthetic iris images for two main reasons: on the one hand, this avoids any possible overlap between the reconstructed images and those used in the reconstruction process (which could lead to overoptimistic results), and, on the other hand, it avoids the need for using real iris images in the reconstruction method.

As a consequence, two databases, one containing real iris samples and another containing synthetic samples, are used in the experiments:

- The iris images to be reconstructed are taken from the real database: Biosecure DB, described in Sect. 3.4.6.1
- The synthetic dataset (SDB) is used for the initialization of the reconstruction algorithm (see Fig. 4.10).

Being SDB a database that contains only fully synthetic data, it is not subjected to any

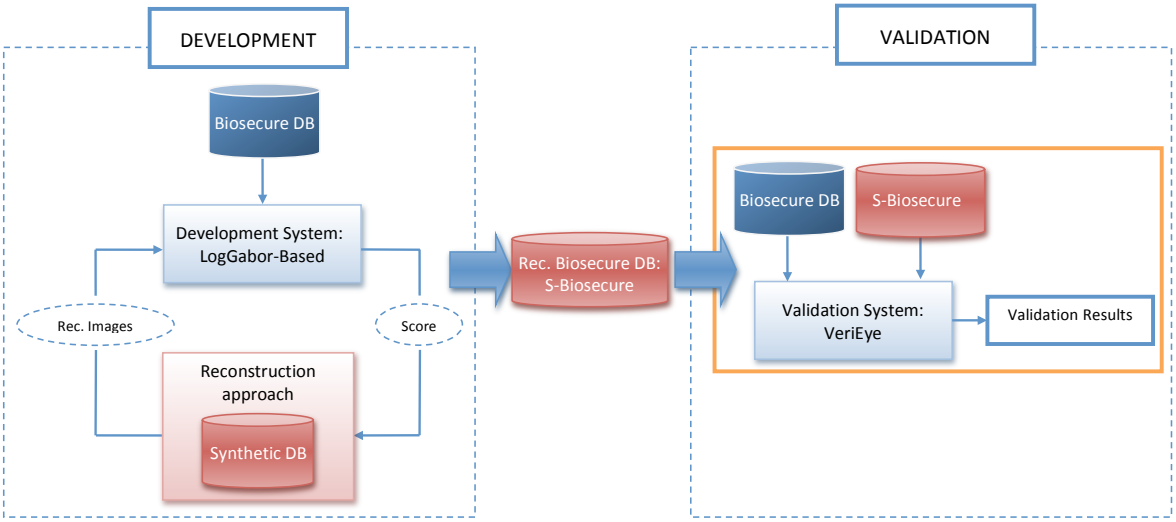


Figure 4.10: *Two-stage experimental protocol followed in the iris-based verification evaluation: i) in the development stage, the GA parameters (population size, mutation probability and block size) are trained on the synthetic DB, and a reconstructed database is generated (S-Biosecure), and ii) in the validation stage, the privacy threat posed by the reconstructed samples is evaluated on a commercial verification system. Real databases are depicted in blue, and synthetic databases in red.*

legal constraints and is publicly available through the CITeR research center[1]. In particular, the synthetic irises are generated following the method described in [Shah and Ross, 2006], which has two stages. In the first stage, a Markov Random Field model is used to generate a background texture representing the global iris appearance [Makthal and Ross, 2005]. In the next stage, a variety of iris features such as radial and concentric furrows, collarette and crypts, are generated and embedded in the texture field. The database includes seven grey-scale images of 1,000 different subjects.

Similarly, two different iris matchers are used in the experiments (see Fig. 4.10):

- The first one, consisting of fully accessible software modules, is used as the development system for the reconstruction of the iris images [Masek and Kovesi, 2003], and is described in Sect. 3.3.2.1.

- The second one, a commercial system completely different from the previous one, is used in the validation stage in order to match the reconstructed images against the real ones [Neurotechnology], and is described in Sect. 3.3.2.2.

Being VeriEye a commercial system, no details on the feature extraction process are provided. Therefore, the results of our proposed method are ensured to be unbiased and not due to a specific adaptation of the reconstruction algorithm to a given validation system.

[1] http://www.citer.wvu.edu/

4.2.2.1. Development Experiments: Reconstructing Images

The objectives of this first set of experiments are: *i*) to fix the values of the different parameters involved in the reconstruction algorithm and, *ii*) once the parameters have been set, to reconstruct the real iris images in Biosecure DB starting from their iriscodes.

In order to achieve these two goals, one sample of each of the 420 subjects present in the Biosecure DB (right and left irises of 210 subjects, see Sect. 3.4.6.1) were randomly selected and their iriscode computed according to the publicly available iris recognition system developed by Masek [Masek and Kovesi, 2003]. The dimensions of the normalized iris images produced by this system are $R \times C = 20 \times 240$ and the size of their corresponding binary templates $K \times W = 20 \times 480$ (i.e., each pixel is coded with two bits).

In order to determine the parameter values of the genetic algorithm effectively, certain general guidelines should be taken into account. Probably, the key factor is to determine the population size. On the one hand, if it is too small the risk of converging prematurely to a local minima is increased since the population does not have enough genetic material to sufficiently cover the problem space (i.e., the diversity is too low). On the other hand, a larger population has a greater chance of finding the global optimum at the expense of drastically increasing the computation load (i.e., CPU time) as the number of iterations needed for convergence is greater.

In most GA-related solutions, the individual's size (i.e., number of blocks $H \times L$) is determined by the problem at hand. However, in our specific case, the same reasoning used for the population size applies to the individual's dimensions as well. Therefore, for this particular problem, a good balance must be obtained between both parameters. As a general rule of thumb, in this specific case, good results are usually obtained when $k \simeq L$.

Besides the aforementioned trade-off, in most GA-related problems the mutation probability is usually kept below 1% in order to avoid losing diversity.

With these general principles in mind, extensive experiments were undertaken to determine a good set of parameter values for the reconstruction algorithm, resulting in the following efficient operating point: population size $k = 80$, mutation probability $p_m = 0.003$, and block size $R/H \times C/L = 2 \times 2$ pixels (i.e., each normalized image is divided into $H \times L = 10 \times 120$ blocks).

It must be emphasized that these parameter values could be further optimized. Furthermore, different strategies than those used here may be adopted in order to implement each of the four rules described in Sect. 4.1.2 (i.e., elite, selection, crossover and mutation). However, the above (or other) improvements related to genetic algorithms are outside the scope of the Dissertation, which is not focused on the study and optimization of this search tool, but rather on the evaluation of the security and privacy of biometric recognition systems, and, in this particular chapter, on the irreversibility analysis of unprotected templates. For a more detailed description of different architectures for genetic algorithms the reader is referred to [Goldberg, 2002, 1989].

Once the parameter values of the reconstruction method were determined and fixed, Masek's matcher [Masek and Kovesi, 2003] was used to compute the matching scores needed by the optimization algorithm, in order to generate 5 different reconstructed images of each binary template

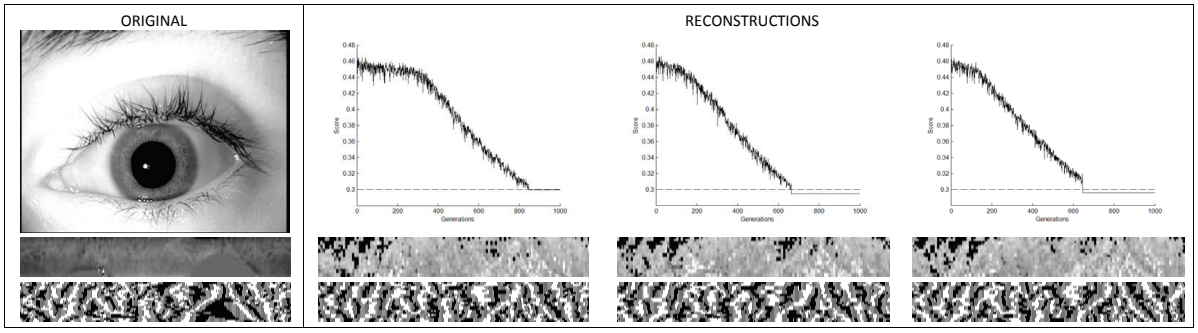


Figure 4.11: *Three example executions (right) of the reconstruction algorithm for the same original image (left). For the reconstruction samples, the evolution of the score through the generations is shown on top (positive matching threshold marked with a horizontal dashed line), with the final reconstructed normalized image and its corresponding iriscode shown below.*

(i.e., the algorithm was applied 5 times to reconstruct and image from each iriscode), thus leading to a database of $5 \times 420 = 2,100$ reconstructed iris images (referred to as Reconstructed Biosecure DB in Fig. 4.10).

In order to determine the positive matching threshold δ at which an iriscode is considered to have been successfully reconstructed, the iris recognition system accuracy was analysed on the Biosecure DB. Mated scores were computed by matching the first sample of each subject to the other 3 images of that same subject (i.e., $420 \times 3 = 1,260$ mated scores), while non-mated scores were generated by comparing the first iris of each subject to the first sample of the remaining subjects in the database (i.e., $420 \times 419 = 175,980$ non-mated scores).

In Fig. 4.11 three different reconstruction outcomes corresponding to a single real iriscode are shown. Although the reconstructed patterns do not visually resemble the original one and block artifacts are discernible, their corresponding iriscodes are all very similar to each other and exhibit a high degree of resemblance with the original. The visual dissimilarity between the original and the reconstructed patterns may be explained by the absence of amplitude-related information in the iriscodes. This leads to arbitrary amplitude values in the synthetically generated samples which, nevertheless, present comparable phase information, resulting in accurate iriscode reproductions. Above each reconstructed image in this figure, the evolution of the score across iterations is shown. Marked with a horizontal dashed line is the positive matching threshold δ.

4.2.2.2. Validation Experiments: Attacking Unprotected Systems

The iris images reconstructed in the development stage are now used to test the vulnerabilities of the VeriEye iris matcher (see the validation chart in Fig. 4.10). As mentioned in Sect. 3.3.2.2, this system operates as a black-box, i.e., given an input, it returns an output with no information about the internal algorithms used to get that final result. Several remarks have to be made regarding the inputs and outputs of VeriEye:

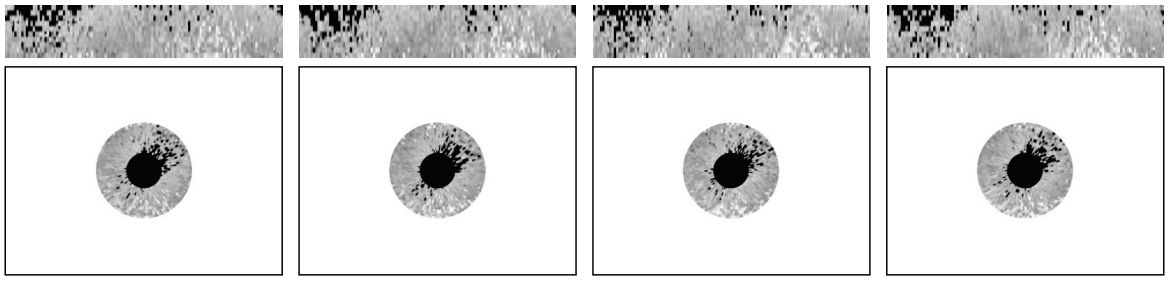


Figure 4.12: *Four reconstructed iris images in pseudo-polar coordinates (top) all recovered from the same original iris, and their corresponding denormalized images in cartesian coordinates used to attack the VeriEye commercial matcher (bottom).*

- *Inputs.* Normalized iris samples in polar coordinates are not accepted by VeriEye. The input to the system has to be an image containing a *circular* iris in cartesian coordinates. For this reason, in order to attack the system, all the reconstructed irides were reconverted into Cartesian coordinates as shown in Fig. 4.12.

- *Outputs.* The system outputs a non-zero similarity score in case of a positive match. When the matching threshold is not reached, a 0 is returned, thereby making it difficult to launch a hill-climbing attack [Gomez-Barrero *et al.*, 2012b]. In case an error occurs during the recognition process (most likely during the segmentation stage), a negative score value is returned.

As was mentioned before, this commercial matcher does not return non-mated scores (i.e., they are always 0) which means that its FMR may not be statistically computed on a given database. In order to fix the threshold for the different operating points, a deterministic equation is given in the documentation enclosed with the system.

In the experiments, the system was unable to segment (i.e., reported an error) 1.4% of the real images in the Biosecure DB. This implies that, for these cases, a sample from a legitimate subject would have not been able to access the system. Thus, the highest SR that can be reached by the attacks is 98.6%. Moreover, 0.5% of the reconstructed images were not correctly segmented (these are regarded as unsuccessful attacks).

As in the previous case study, the performance of the attacks is measured in terms of its Success Rate (SR), which is defined as the expected probability of bypassing the attacked system (see Sect. 3.2). Table 4.12 shows a summary of the total number of attacks carried out for each experiment and database, where sub-indices denote the attack under consideration. Furthermore, SR will be computed at three operating points corresponding to: FMR = 0.1%, FMR = 0.05%, and FMR = 0.01%, which, according to [ANSI/NIST, 2009], correspond to a low, medium and high security application, respectively. For completeness, the system is also tested at a very high security operating point corresponding to FMR $\ll$ 0.01%.

Table 4.12: *Total number of attacks carried out for each experiment for the iris case study.*

	Biosecure DB
A_{T1a}	$420 \times 5 = 2,100$
A_{T1b}	$420 \times 5 \times 3 = 6,300$
A_{T2a}	420
A_{T2b}	$420 \times 3 = 1,260$
A_{T3}	420

Table 4.13: *SR of the different attacking scenarios considered for the VeriEye matcher at the four operating points tested.*

FMR	SR(%) - VeriEye					
	SR_{1a}	SR_{1b}	SR_{2a}	SR_{2b}	SR_3	**Average**
0.1%	81.2	66.7	96.2	92.8	96.7	**86.7**
0.05%	79.2	63.4	96.2	91.4	95.2	**85.1**
0.01%	77.3	60.9	95.2	90.9	93.8	**83.6**
0.0001%	69.0	49.1	92.8	82.8	82.9	**75.3**

Several observations can be made from the results of the validation experiments carried out on VeriEye as shown in Table 4.13:

- The high performance of the proposed reconstruction algorithm is confirmed, reaching an average SR of around 85% for the three usual operating points considered, and over 95% for the most likely attacking scenario (i.e., SR_{2a}).
- Even for an unrealistically high security point (i.e., FMR=0.0001%), the reconstructed images would have, on average, almost 75% chances of breaking the system.
- As expected, it is more probable that the synthetic samples are positively matched to the original image from which they were reconstructed than to other real images of the same subject (see the decrease in the SR between SR_{1a} *vs* SR_{1b} and between SR_{2a} *vs* SR_{2b}).
- Even so, the reconstructed images still present a high probability of breaking the system even when the stored templates are not the one from which they were recovered (average SR of SR_{1b} and SR_{2b} around 75%).
- Furthermore, in the case of using several real samples of the subject for verification (SR_3), the reconstructed images are still able to access the system ∼94% of the time at the usual operating points, and 80% of the time in the extremely high operating point tested.

Table 4.14: *Percentage of successful attacks where n out of the total 5 reconstructed images were positively matched against the original iris image from whose iriscode they were reconstructed. Results are given for the four operating points tested on VeriEye.*

FMR	$\mathbf{SR}_n$ (%) - VeriEye				
	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$
0.1%	1.9	5.3	13.3	24.8	50.9
0.05%	2.4	6.7	13.8	27.6	45.7
0.01%	3.8	6.2	13.8	28.1	43.3
0.0001%	7.6	6.7	21.9	24.7	31.9
Average	3.9	6.2	15.7	26.3	42.9

- Besides, a new possible vulnerability of iris recognition applications has been raised, as the tested matcher positively matches images with a black circle in the middle and a white background (such as the ones shown in Fig. 4.12) that should by no means be recognized as an eye image.

The last observation emphasizes the need for incorporating some type of pre-checking stage, prior to the localization and segmentation of the iris, in order to confirm that the sample presented to the system is really that of an eye, and not some simple iris-like image.

The results presented in Table 4.13 confirm the first and second objectives set in the present chapter: iris images may be recovered from their iriscodes, and the reconstructed images represent a real threat to the integrity of automatic recognition systems. In other words, unprotected templates are reversible, hence putting the privacy of the subject at risk.

Recall now that the third goal of the study is to determine the feasibility of generating multiple synthetic iris patterns with iriscodes very similar to a real one. In order to address this point, results from experiment 2.a (i.e., all 5 synthetic images are compared to the original image) are presented in Table 4.14 from a different perspective. In this case we report in each column the percentage of attacks in which only n out of the 5 reconstructed images (with $n = 1, \ldots, 5$) were positively matched to the original real image. In each case, the total number of attacks performed is $A_{Tn} = 420$ and the success rate is denoted as SR_n.

Averaging over the four operating points, all five reconstructed images were positively matched to the original image in 42.9% of the cases. This increases to 69.2% if we consider $n = \{4, 5\}$, and to 84.9% when taking into account $n = \{3, 4, 5\}$. These results confirm the ability of the proposed probabilistic reconstruction method to generate multiple iris patterns which are positively matched to one specific iriscode. As can be seen in Table 4.13, this ability gives the proposed method a much higher attacking potential than deterministic algorithms that can only generate one image from each iriscode: the success rate increases by around 27% on an average when several reconstructions of the iris image are available (i.e., attack 2: $1 vs 5$)

compared to the case in which only one reconstructed sample is used to access the system (i.e., attack 1: $1vs1$).

4.3. Chapter Summary and Conclusions

In this chapter we have introduced two novel algorithmic methods for the reconstruction of synthetic biometric samples, which are positively matched to the reference templates extracted from real biometric data. The first method relies on the combination of a handshape images generator and the Uphill Simplex algorithm to optimize its input. The second makes use of a genetic algorithm to optimize normalised gray-scale iris images. The security and privacy threat entailed by such synthetic samples has been later analysed within the general framework presented in Chapter 3 for the evaluation of unprotected systems, and, more specifically, the irreversibility analysis of the templates.

Both reconstruction methods assume that *i*) the system stores unprotected templates (or the attacker is able to override this protection) and *ii*) the attacker has access to the scores produced by a development system between the referenced template and several synthetic samples. It may be hence argued that attacks such as the ones considered in this chapter can be successful only when the reference template is compromised. This may be difficult (although possible) in classical biometric systems where the enrolled templates are kept in a centralized database. In this case, the attacker would have to access the database and extract the information, or intercept the communication channel when the stored template is released for matching. But the threat is heightened in Match-on-Card (MoC) applications where an individual's biometric template is stored in a smartcard possessed by the person. Such applications are rapidly growing due to several appealing characteristics such as scalability and privacy [Bergman, 2008b]. Similarly, biometric data is being stored in many official documents such as the new biometric passport [ICAO, 2006], some national ID cards [Government of Spain], the US FIPS-201 Personal Identity Verification initiatives (PIV) [NIST] and the ILO Seafarers Identity Card Program [ILO, 2006]. In spite of the clear advantages that these type of applications offer, templates are more likely to be compromised as it is easier for the attacker to have physical access to the storage device and, as has already been demonstrated [van Beek, 2008], fraudulently obtain the information contained inside. This makes MoC systems potentially more vulnerable to the type of threat described in this chapter especially when the biometric data is stored without any type of protection [NIST], or printed in the clear on plastic cards as 2D barcodes [ILO, 2006].

Assuming such knowledge (i.e., the attacker can obtain the similarity score between the reference template and several reconstructed images), the experimental evaluation has shown that the information summarized in handshape and iris templates is sufficient to generate synthetic images with very similar templates to those of the original biometric samples. The experimental findings indicate that an eventual attack to biometric systems using such reconstructed images would have a very high chance of success, hence violating the privacy of the subjects.

It should be noted that the methods proposed are not specific for the systems evaluated.

On the one hand, different biometric systems, relying on independent features, have been used to generate and validate the reconstructed samples. On the other hand, since they require no knowledge about the templates' format, they can be potentially used to reconstruct samples from templates based in a different set of features. In addition, the experimental findings have also shown that, given the probabilistic nature of the optimization algorithms used, not only one but several synthetic samples can be generated from a single template. This not only significantly increases the success rate of the attacks compared to methods that can generate only one synthetic sample, but it also opens up the possibility of other applications besides inverse biometrics, such as to increase the amount of available data of a subject.

As a consequence of the high success chances inverting the templates to the original biometric samples, the work presented in this chapter has reinforced the need for including template protection schemes in commercial systems. If unprotected templates are stored or used at any time for verification purposes, it has been proven that the information comprised is enough to successfully reconstruct synthetic images which are positively identified as genuine samples. Furthermore, such positive matches are carried out by other independent systems, not necessarily the ones used for the reconstruction. With such reconstructed samples, an eventual attacker could impersonate a particular subject, hence constituting a severe privacy threat. This fact has motivated the development of adequate biometric template protection schemes in the following chapters.

Novel contributions of this chapter are:

- Two inverse biometrics methods for the reconstruction of handshape and iris samples, based on optimization algorithms.
- The systematic evaluation of the security and privacy of unprotected templates for three handshape based systems and a commercial iris system using the reconstructed synthetic samples.

Chapter 5

Biometric Template Protection Based on Bloom Filters

In this chapter we present a generic Biometric and Multi-Biometric Template Protection scheme based on Bloom filters to deal with the privacy issues unveiled in Chapter 4. Then, we evaluate it in terms of accuracy, irreversibility, unlinkability and robustness to cross-matching attacks, in accordance with the security and privacy evaluation protocol established in Chapter 3, Sect. 3.2, and with the requirements established in the ISO/IEC 24745 International Standard on biometric information protection [ISO/IEC JTC1 SC27 IT Security Techniques, 2011].

As indicated in Chapter 2, even though Bloom filter based template protection offers fast and accuracy-preserving biometric verification, some concerns have been raised regarding the unlinkability of the templates. Additionally, although schemes for different characteristics have been proposed, the main parameters for the Bloom filter computation have to be specifically devised for each case study.

In this Chapter, we present two different protection schemes:

- An unlinkable and irreversible biometric template protection scheme based on Bloom filters.
- A general multi-biometric template protection scheme based on a weighted feature level fusion.

Furthermore,

- We propose a methodology for estimating the appropriate parameters for the Bloom filter based template computation.

In a reproducible research framework, two sets of experiments are carried out on independent and publicly available databases in order to avoid biased results. First, the parameters of the Bloom filter template computation are estimated on the development databases. Then, the security and privacy of the schemes is evaluated on the test databases. In a first stage, the

verification accuracy is analysed for several case studies (face, iris, fingerprint, fingervein and a face and iris fusion). At a second stage, the irreversibility, unlinkability and robustness to cross-matching attacks are systematically analysed for the face based scheme.

The chapter is structured as follows. Sect. 5.1 gives a brief introduction to the original Bloom filter based BTP and describes the proposed systems, with one subsection dedicated to each of them: Sect. 5.1.1 describes the novel unlinkable and irreversible template protection scheme based on Bloom filters, Sect. 5.1.2 presents the methodology for the parameter estimation, Sect. 5.1.3 describes the new multi-biometric template protection scheme based on Bloom filters and Sect. 5.1.4 summarises potential attacks to Bloom filter based schemes. Then all schemes are evaluated on Sect. 5.2. First, appropriate parameters are estimated for four different case studies (face, iris, fingerprint and fingervein) in Sect. 5.2.1 and the obtained accuracy is evaluated in Sect. 5.2.2. Then, for the face case study, irreversibility is analysed in Sect. 5.2.3, unlinkability in Sect. 5.2.4 and robustness to cross-matching attacks in Sect. 5.2.5. The chapter summary and conclusions are presented in Sect. 5.3.

This chapter assumes a basic understanding of the fundamentals of pattern recognition [Duda *et al.*, 2001; Theodoridis and Koutroumbas, 2008], and image processing [Gonzalez and Woods, 2006].

This chapter is based on the publications: [Gomez-Barrero *et al.*, 2016d,e, 2014c; Rathgeb *et al.*, 2015].

We will use the following notation throughout the Chapter:

- $\mathbf{T}_p$ and $\mathbf{T}_r$: probe and reference unprotected templates.
- $|\mathbf{T}|$: unprotected template size.
- $\mathbf{b}$: Bloom filter.
- $|\mathbf{b}|$: number of bits activated, or set to one, in a Bloom filter.
- *nBlocks*: number of blocks into which the unprotected template is divided.
- *nWords* and *nBits*: dimensions of the aforementioned blocks, corresponding to the number of words inserted into the corresponding Bloom filter (*nWords*), and length of such words (*nBits*).
- $\mathbf{C}_p = \{\mathbf{b}_1, \ldots, \mathbf{b}_{nBlocks}\}$: cancelable template corresponding to $\mathbf{T}_p$, and comprising *nBlocks* Bloom filters.
- S_{BF}: similarity score between two cancelable templates corresponding to $\mathbf{C}_p$ and $\mathbf{C}_r$, computed according to Eq. 5.2.
- *nSeq*: number of possible sequences, or unprotected templates $\mathbf{T}$, which yield the same protected template $\mathbf{C}$.

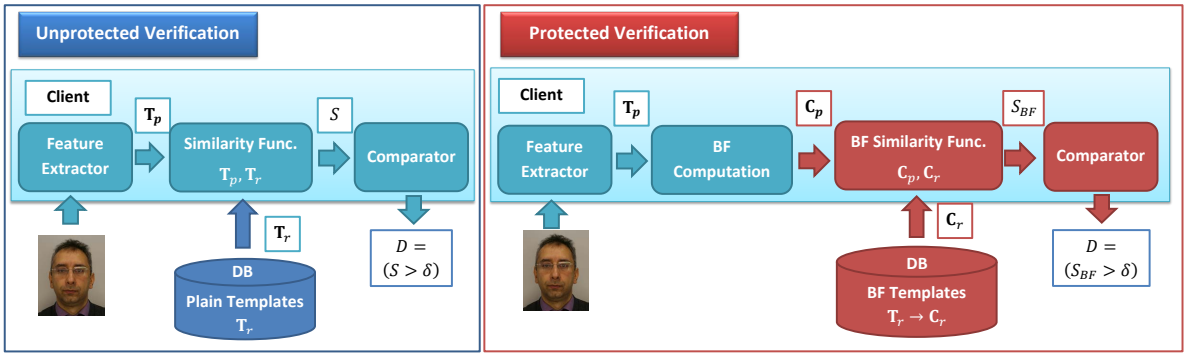


Figure 5.1: Unprotected vs Protected Biometric Verification. *In the unprotected scenario (left), a probe biometric sample is acquired and its features extracted ($\mathbf{T}_p$). The similarity score with respect to the probe reference $\mathbf{T}_r$ is computed, $S = d(\mathbf{T}_p, \mathbf{T}_r)$, and the final output is the mated/non-mated decision $D = (S > \delta)$. In the protected scenario (right), all the protected data or information flow is depicted in red: $\mathbf{C}_p$, $\mathbf{C}_r$ and S_{BF}. In this case, an additional module is added to compute the protected templates, $\mathbf{C}_p$ (more details in Fig. 5.2), and a different distance function, specific for the Bloom filter templates, is used (see Eq. 5.2).*

- $\mathbf{K}_{trans}$: secret key for the structure-preserving feature transformation or for the weighted feature level fusion, with $trans \in \{perm, \texttt{XOR}\}$.
- $|\mathbf{K}|$: key space size.
- p_{nWords}: probability of activating one particular bit within a Bloom filter, after inserting $nWords$ words.

5.1. Biometric Template Protection Based on Bloom Filters

In general, biometric verification involves the following steps, as depicted in Fig. 5.1 (left):

- Feature extraction: the probe biometric sample is acquired and features extracted and encoded in the probe template $\mathbf{T}_p$.
- Similarity score computation: the similarity score S between the probe $\mathbf{T}_p$ and reference $\mathbf{T}_r$ templates, stored in a possibly external database, is generated.
- Comparison: the final mated/non-mated verification decision $D = (S > \delta)$ is computed, where δ is the pre-defined verification threshold.

As shown in Chapter 4, the storage and comparison of unprotected templates raises severe security and privacy issues due to the possible information leakage. To tackle them, cancelable biometric approaches irreversibly transform the unprotected templates $\mathbf{T}$ into protected references $\mathbf{C}$ by adding a new module, and, if necessary, modifying the similarity score computation function. In particular, for Bloom filter based BTP schemes, the following steps are undertaken (see Fig. 5.1, right):

- Feature extraction: the probe biometric sample is acquired and features extracted and encoded in the probe template $\mathbf{T}_p$.
- Bloom filter computation: the protected biometric template, $\mathbf{C}_p$, is computed from its unprotected counterpart, $\mathbf{T}_p$, which is automatically discarded.
- Similarity score computation: the similarity score S_{BF} between the probe $\mathbf{C}_p$ and reference $\mathbf{C}_r$ templates, stored in a possibly external database, is generated.
- Comparison: the final mated/non-mated verification decision $D = (S_{BF} > \delta)$ is computed, where δ is the pre-defined verification threshold.

For the Bloom filter based template computation, initially introduced for iris verification, Rathgeb *et al.* [2013a] propose to divide the binary iriscode into *nBlocks* blocks comprising $nBits \times nWords$ bits. From each such block, one Bloom filter, $\mathbf{b}$, of length 2^{nBits} is computed - the final cancelable template is thus composed of *nBlocks* Bloom filters. In order to extract a Bloom filter from a given binary block, columns (denoted as *words*) are mapped to their decimal value, and the corresponding index in $\mathbf{b}$ - initially set to zero - is set to one. Each bit can be thus set to one multiple times, but only the first change has an effect, thereby achieving irreversible templates. In this original approach, the authors propose to `XOR` the columns with secret keys before activating the corresponding bits in the Bloom filter in order to achieve unlinkability. However, it has been proven that templates are still linkable [Bringer *et al.*, 2015; Hermans *et al.*, 2014]. To avoid such privacy violation, in the next section we propose an improved Bloom filter BTP scheme.

5.1.1. Irreversible and Unlinkable Biometric Template Protection

A diagram of the proposed improved Bloom filter based BTP scheme is depicted in Fig. 5.2. In contrast to the original concept, an additional processing step, referred to as *Structure-preserving feature re-arrangement*, is introduced (highlighted in red in Fig. 5.2). Hence, the improved scheme comprises three key components:

1. *Feature extraction*: in the first step, an unprotected two-dimensional binary feature vector is extracted from the biometric samples, e.g. facial image. In the same way as in the original concept, the binary feature vector is divided into *nBlocks* blocks of size $nBits \times nWords$ bits, as shown as part of Fig. 5.2.

2. *Structure-preserving feature re-arrangement*: the goal of this processing step is to dissipate the statistical composition of the biometric feature vector. In order to maintain recognition accuracy, a certain structure of words within feature blocks has to be retained. Otherwise, stability of discriminative words is lost prior to the computation of Bloom filters. In order to reach a balance between verification accuracy and diffusion of feature vectors, we first re-group the *nBlocks* blocks into *nGroups* sets of B blocks ($nBlocks = nGroups \times B$, see Fig. 5.2).

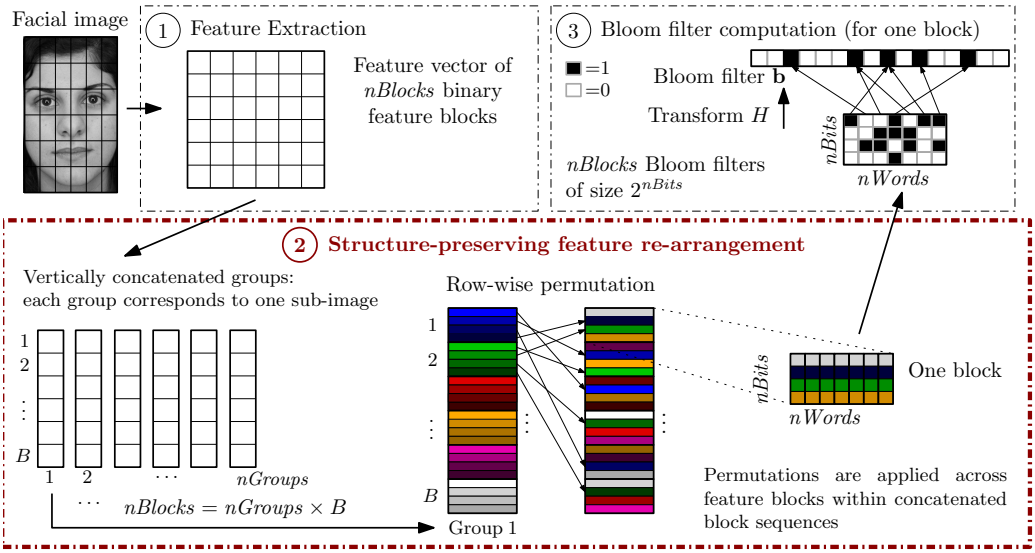


***Figure 5.2: System overview**: 1) a binary feature vector consisting of nBlocks binary feature blocks of size nBits × nWords is extracted; 2) the entire set of blocks is disposed into nGroups vertically concatenated groups consisting of B blocks, and structure-preserving feature re-arrangement is applied; 3) a total number of nBlocks Bloom filters is extracted (one for each transformed feature block).*

Within such groups of blocks, a *row-wise permutation* (*perm*) is performed: for each of the *nGroups* sets, the rows of the vertical concatenation of the corresponding B blocks are permuted. Note that a permutation of columns would not cause any change in the resulting Bloom filters, since changing the order of insertion of the words into the Bloom filter makes no difference in the final output. Due to the fact that horizontal neighbourhoods of bits within rows persist, this sub-step prevents from a potential loss of discriminative power of resulting feature blocks. On the other hand, the dissipation of rows among groups of blocks significantly improves the information diffusion and prevents block-based attacks. In case of a permutation within feature blocks, a potential attacker, which has full knowledge of the employed permutation key (full disclosure model), would be able to revert Bloom filters to feature blocks separately after applying the reverse permutation, which involves an arrangement of $|\mathbf{b}|$ words to a block of length *nWords* with *nSeq* possible sequences of words (see below, Eq. 5.4). However, applying an inverse permutation across a group of blocks prior to reverting Bloom filters to feature blocks is not feasible, since without loss of generality, the number of activated bits in Bloom filters of feature blocks of one group differs. This means that, after applying the correct inverse permutation adjacencies of bits forming each word are potentially lost. As a consequence, one out of *nSeq* sequences would have to be guessed for each of the B blocks of a group, prior to applying the inverse permutation. Moreover, the re-grouping of feature blocks increases the size of the key space for the applied permutation.

3. *Bloom filter computation*: in the final step one Bloom filter is computed from each of the *nBlocks* blocks, such that the final protected template $\mathbf{C}$ consist of *nBlocks* Bloom filters

of size 2^{nBits}. An example of this processing step for a single feature block is shown as part of Fig. 5.2. All the bits in the corresponding Bloom filter $\mathbf{b}$ are initially set to zero. Then, each binary word $\mathbf{w}_i = \{w_i[1], \ldots, w_i[nBits]\}$ (i.e., a column within the feature block) is translated into its corresponding decimal value, $H(\mathbf{w}_i)$, for $i = 1, \ldots, nWords$. Subsequently, the bits corresponding to those decimal values are activated in $\mathbf{b}$:

$$\mathbf{b}[H(\mathbf{w}_i)] = 1 \text{ with } H(\mathbf{w}_i) = \sum_{j=1}^{nBits} w_i[j] \cdot 2^{j-1} \tag{5.1}$$

This operation is repeated for each of the *nBlocks*, in order to obtain the final protected template $\mathbf{C} = \{\mathbf{b}_1, \ldots, \mathbf{b}_{nBlocks}\}$, where the length of each $\mathbf{b}$ is 2^{nBits}.

The final comparison score S_{BF} between a probe and a reference cancelable templates, $\mathbf{C}_p$ and $\mathbf{C}_r$, is then defined as the average Bloom filter dissimilarity score:

$$S_{BF} = PIC(\mathbf{C}_p, \mathbf{C}_r) = \frac{1}{nBlocks} \sum_{i=1}^{nBlocks} \frac{HD(\mathbf{b}_p^i, \mathbf{b}_r^i)}{|\mathbf{b}_p^i| + |\mathbf{b}_r^i|} \qquad |\mathbf{b}_p^i| + |\mathbf{b}_r^i| \neq 0 \tag{5.2}$$

where $|\mathbf{b}|$ denotes the number of bits within a Bloom filter $\mathbf{b}$ set to 1, and $HD(\mathbf{b}_p^i, \mathbf{b}_r^i)$ the Hamming distance between two Bloom filters.

Within the presented scheme, irreversibility is achieved by mapping column-wise words to Bloom filters. Given a Bloom filter $\mathbf{b}$ of length 2^{nBits} we restrict to inserting only $nWords$ words, where $nWords \leq 2^{nBits}$ (blocks do not contain more than 2^{nBits} columns). In case of uniformly distributed data, the probability that a certain bit is set to 1 during the insertion of an element is $1/2^{nBits}$. Conversely, the probability that a bit is still 0 is $1 - 1/2^{nBits}$. As a consequence, after inserting a total of $nWords$ words, and under the uniformity assumption, the probability that a particular bit is activated, p_{nWords}^{uni}, is

$$p_{nWords}^{uni} = 1 - \left(1 - \frac{1}{2^{nBits}}\right)^{nWords} \tag{5.3}$$

However, focusing on biometric data this theoretical expectation does not apply, since bits of binary biometric feature vectors must not be expected to be mutually independent (i.e. reasonable parts of feature vectors correlate). Consequently, a significant number of words is expected to be mapped to identical positions in Bloom filters even for small values of $nWords$. Let us assume $|\mathbf{b}|$ bits are set to 1 within a Bloom filter after inserting $nWords$ words, i.e. $|\mathbf{b}|$ different words occur in a block of $nWords$. Hence, the probability of re-mapping a bit to a certain position is $1 - |\mathbf{b}|/nWords$. For a potential attacker the reconstruction of the original template part involves arranging $|\mathbf{b}|$ words to $nWords$ positions. For $|\mathbf{b}| \leq nWords$ the theoretical number of possible sequences is recursively defined by $nSeq$ as a function of $|\mathbf{b}|$ and $nWords$, where each of the $|\mathbf{b}|$ words have to appear at least once within $nWords$ columns,

$$nSeq(|\mathbf{b}|, nWords) = \begin{cases} 1, & \text{if } |\mathbf{b}| = 1 \\ |\mathbf{b}|^{nWords} - \sum_{i=1}^{|\mathbf{b}|-1} \binom{|\mathbf{b}|}{i} \cdot nSeq(i, nWords) & \text{otherwise} \end{cases} \tag{5.4}$$

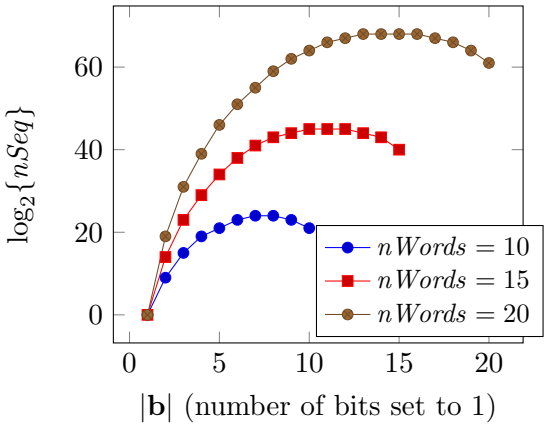


Figure 5.3: *Number of possible sequences nSeq (per block) for different block sizes and proportions of re-mapped codewords.*

In other words, all sequences with less than $|\mathbf{b}|$ words are subtracted from the number of all possible sequences, $|\mathbf{b}|^{nWords}$.

Fig. 5.3 illustrates the rapid increase of possible sequences even for small values of $|\mathbf{b}|$ (note the logarithmic scale in the y axis). Peaks are located around $3/4 \cdot nWords$, and in the extremes we get $nSeq\,(nWords, nWords) = nWords!$ and $nSeq\,(1, nWords) = 1$. For example: for $nWords = 4$ and $|\mathbf{b}| = 2$ we get $nSeq(2,4) = 2^4 - \binom{2}{1} \cdot nSeq(1,4) = 16 - 2 \cdot 1 = 14$ possible sequences, for $nSeq = 4$ and $|b| = 3$ we get $nSeq(3,4) = 3^4 - \binom{3}{1} \cdot nSeq(1,4) - \binom{3}{2} \cdot nSeq(2,4) = 81 - 3 \cdot 1 - 3 \cdot 14 = 36$ possible sequences, for $nWords = 4$ and $|\mathbf{b}| = 4$ we get $nSeq(4,4) = 4! = 24$ possible sequences and so forth.

Regarding unlinkability, it could be argued that despite the proposed structure-preserving feature re-arrangement, a random shuffling of bits would fulfil the task of dissipating the statistical composition of the biometric feature vector. However, such an approach significantly affects verification accuracy, as will be shown in the experiments. Alternatively, `XOR`-ing the entire feature vector with a randomly generated binary vector of the same size (one-time pad) could be considered. However, while such an approach would achieve sufficiently large key spaces, block-based attacks could be employed in a scenario where an attacker has full knowledge of the applied key, since biometric information would not be dispersed across feature blocks prior to the Bloom filter computation.

It should be finally noted that the level of unlinkability and irreversibility achieved by the proposed system will be influenced by the size of the key space, $|\mathbf{K}|$, of the considered structure-preserving feature re-arrangement. Two facts should be taken into account for the computation of $|\mathbf{K}|$: *i*) the dimensions of feature blocks and concatenated groups of blocks to which the *perm* transform is applied, and *ii*) the number of feature blocks and concatenated groups of blocks, since different keys are applied for each of these. In our particular approach, we are carrying out $nGroups$ different permutations (one for each group of blocks) of $nBits \times B$ rows. Therefore,

for each permutation we have $(nBits \times B)!$ different keys resulting in,

$$|\mathbf{K}| = (nBits \times B)!^{nGroups} \tag{5.5}$$

In contrast to the original approach [Rathgeb *et al.*, 2013a], key space sizes of the proposed structure-preserving feature re-arrangement are large enough to prevent brute force cross-matching attacks, as will be shown in the experimental section (Sect. 5.2.5).

5.1.2. Parameter Estimation

As mentioned at the beginning of the chapter, the main challenge in the application of the Bloom filter based template protection scheme described above to a new biometric characteristic lies in determining the size of the feature blocks from which the Bloom filters are computed. That is, finding the appropriate values for *nBits* and *nWords*. In the next sections, a two-step methodology to find appropriate bounds for each parameter are provided based on a statistical analysis of the binary unprotected templates, as depicted in Fig. 5.4.

5.1.2.1. Computation of *nBits*

First of all, we should bear in mind that *nBits* determines the length of the Bloom filters (2^{nBits}). Therefore, small values will lead to small Bloom filters, which will be unable to grant irreversibility: if only a few words are inserted, there will be no collisions and it will be easy to reconstruct the original feature block. On the other hand, if more words are inserted, too many words will be coded into a single bit and verification accuracy will be severely affected. We should hence maximize *nBits*, in order to grant irreversibility, as long as verification accuracy is not compromised.

Intuitively, the more correlations within the binary template, the more information can be coded in a single Bloom filter without losing its discriminative power, thereby preventing accuracy degradation. In order to account for those correlations, we will estimate the Degrees of Freedom (N) of those templates, and compute the upper bound of *nBits* as the ratio between the template size $|\mathbf{T}|$ and N (Fig. 5.4, 1):

$$nBits \leq \frac{|\mathbf{T}|}{N} \tag{5.6}$$

In order to estimate N, we can model the non-mated Hamming Distance (HD) distribution with a binomial distribution with mean p and standard deviation σ [Daugman, 2004]. This is due to the fact that each comparison between two bits from two different binary templates is essentially a Bernoulli trial, where correlations between successive "coin tosses" are a consequence of the existing correlations in the biometric samples. The Degrees of Freedom of the distribution can be hence computed as

$$N = \frac{p\,(1-p)}{\sigma^2} \tag{5.7}$$

Finally, we will choose *nBits* as close as possible to the upper bound estimated in Eq. 5.6, in order to maximize the irreversibility and unlinkability provided by the system.

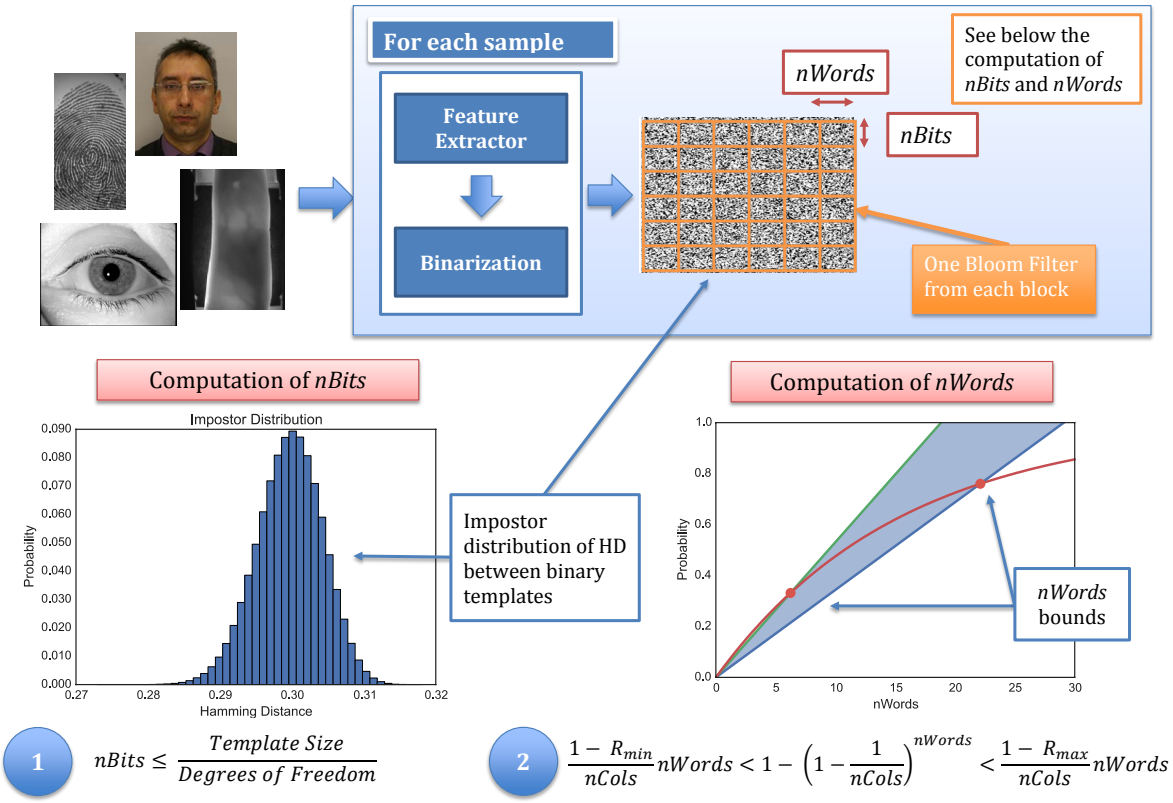


Figure 5.4: General diagram for the parameter estimation *in Bloom filter based template protection schemes. In the first step, an upper bound is computed for nBits based on the Degrees of Freedom of the Hamming distance non-mated distribution of the unprotected templates. Then, that value is used to estimate the appropriate range for nWords, so that verfication accuracy is mantained and irreversibility is achieved.*

5.1.2.2. Computation of $nWords$

While $nBits$ has a direct impact on the template size, $nWords$ influences the number of activated bits within a Bloom filter ($|\mathbf{b}|$). Assuming independence, the probability that one particular bit is activated within a Bloom filter of length 2^{nBits} after inserting $nWords$ columns, p^{uni}_{nWords}, is given by Eq. 5.3. However, as already pointed out, not all words are equally probable due to the correlations existing within the biometric samples. In fact, not even all 2^{nBits} words will appear in a single template if $nBits$ is big enough with respect to the template size. Therefore, we will estimate the average number of different words of length $nBits$ for the unprotected templates, and substitute 2^{nBits} for that average value, $nCols$, giving a better estimation for p_{nWords}:

$$p_{nWords} = 1 - \left(1 - \frac{1}{nCols}\right)^{nWords} \tag{5.8}$$

To establish boundaries for that probability, we will take into account the words re-map rate R, which models the non-independence between the words of each feature block. For a given R,

the probability of activating one particular bit after inserting *nWords* is

$$p_{nWords}(R) = \frac{(1-R)\cdot nWords}{nCols} \tag{5.9}$$

In order to preserve accuracy while granting irreversibility, the re-map rate should remain within a certain interval $[R_{min}, R_{max}]$. This interval should be centred around $R = 0.25$, which is the the optimal value for the re-map rate with respect to irreversibility of templates found in [Rathgeb *et al.*, 2013a]. Therefore, using Eqs. 5.8 and 5.9, we estimate the lower and upper bounds of *nWords* so that the following inequalities hold:

$$\frac{1-R_{min}}{nCols} nWords \leq 1 - \left(1 - \frac{1}{nCols}\right)^{nWords} \leq \frac{1-R_{max}}{nCols} nWords \tag{5.10}$$

The final value for *nWords* will be chosen within the estimated range, taking into account the size of the template, so that: *i*) a sufficient number of Bloom filters can be computed, thereby preserving verification accuracy, and *ii*) choosing a value that divides the total number of columns in the template, in order to minimize the information loss.

In Fig. 5.4 (2) a particular example of those inequalities for $nBits = 4$ and $nCols = 16$ is shown. The shaded area represents the area in which the inequalities hold, and the red curve represents the function to optimize (the central term in Eq. 5.10). The intersections of the red curve with the limits of the shaded area hence determine the approximate range of appropriate values for *nWords*.

5.1.2.3. General Remarks

Some general remarks ought to be made regarding the methodology described for some particular cases.

On the one hand, some verification systems divide the initial sample into sub-images before extracting the features (e.g., the face verification system used in the experiments, see Sect. 3.3.3). In that case, in order to retain all the discriminative information, *nBits* will be estimated for each sub-image and the minimum value will be considered. Then, *nWords* will be subsequently estimated for that sub-image.

On the other hand, when we are dealing with variable length templates (e.g., the fingerprint verification system used in [Li *et al.*, 2015], see Sect. 3.3.5.1), Hamming Distances can not be computed in a straightforward manner. In those cases, given two templates $\mathbf{T}_1$, $\mathbf{T}_2$, with $|\mathbf{T}_1| > |\mathbf{T}_2|$, we will divide each template into its basic units (e.g., minutiae vicinities in [Li *et al.*, 2015]). Then, for each basic unit in $\mathbf{T}_2$, $\mathbf{t}_2^i$, with $i = 1, \ldots, |\mathbf{T}_2|$, we will find the closest unit in $\mathbf{T}_1$, $\mathbf{t}_1^j$, in terms of their Hamming Distance, $HD\left(\mathbf{t}_2^i, \mathbf{t}_1^j\right)$. The final Hamming Distance between the templates can be thus computed as the average *HD* between their basic units:

$$HD(\mathbf{T}_1, \mathbf{T}_2) = \frac{1}{|\mathbf{T}_2|} \sum_{i=1}^{|\mathbf{T}_2|} \min_j HD\left(\mathbf{t}_2^i, \mathbf{t}_1^j\right) \tag{5.11}$$

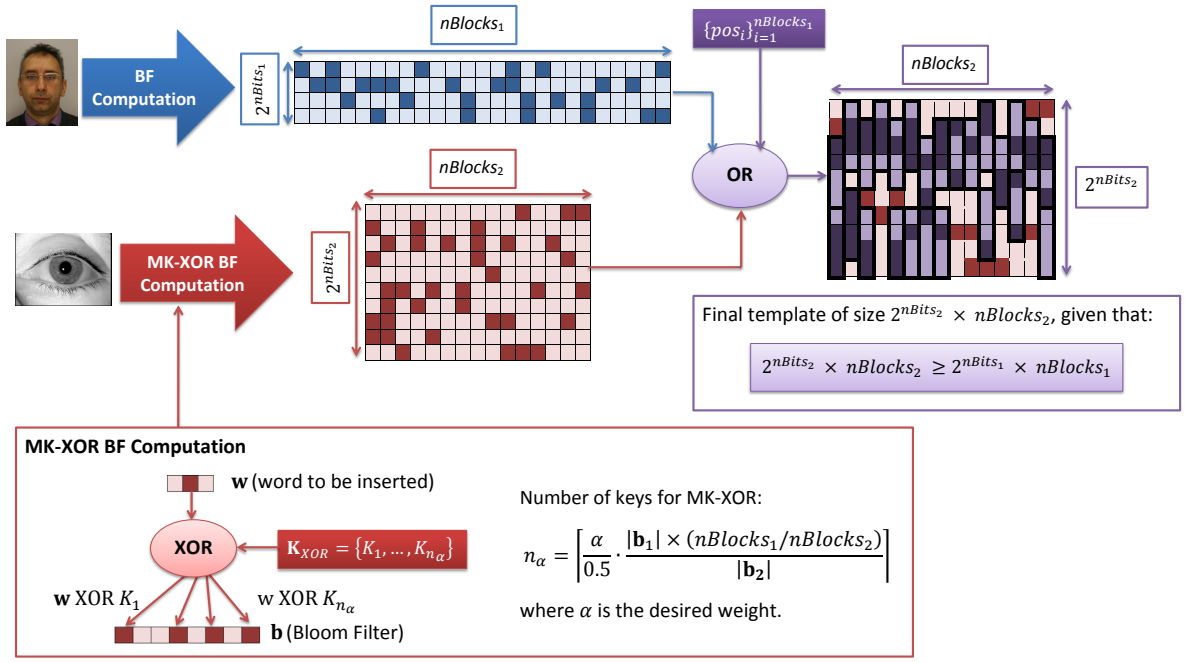


Figure 5.5: General diagram for feature level fusion *in Bloom filter based template protection schemes. The smaller template (in blue) is re-allocated over the bigger one (in red), according to the positions defined by the system (in purple), and they are* OR*ed to obtain the final fused template. Additionally, in order to achieve a weighted fusion, multiple bits are activated with each word* $\mathbf{w}$*, using a Multi-Key XOR (MK-XOR) approach for the Bloom filter computation of one of the fused characteristics.*

Finally, it should be noted that N takes into account all correlations within the template, in both the vertical and horizontal directions. However, in order to estimate an appropriate value for $nBits$, only the former should be taken into account. Therefore, for those unprotected templates presenting correlations in both directions (e.g., the binary iriscode or the Spectral Minutiae Representation), $N/2$ will be used in Eq. 5.6.

5.1.3. Multi-Biometric Template Protection

In order to improve verification accuracy and the level of security and privacy provided, we propose a general weighted feature level fusion for protected templates of possibly different sizes. Firstly, $nBits$ and $nWords$ are estimated for each individual characteristic, according to the methodology proposed in the previous section. Since the proposed fusion technique is based on the OR of Bloom filter based cancelable templates, it can be applied to any number of biometric characteristics. However, for the sake of clarity, we will focus in the two-case scenario.

A general diagram for the proposed scheme is depicted in Fig. 5.5, describing the fusion of two characteristics, whose estimated parameters are $\{nBits_1, nWords_1\}$ and $\{nBits_2, nWords_2\}$. Without loss of generality, let us assume $|\mathbf{T}_2| = 2^{nBits_2} \times nBlocks_2 \geq 2^{nBits_1} \times nBlocks_1 = |\mathbf{T}_1|$ (i.e., the protected template extracted from the second biometric characteristic, in red, is bigger than the first one, in blue). The final fused template is computed as the OR of the individual

protected templates: that way, a bit activated in any of the templates will be in turn activated in the fused template. However, since we consider the general case where $|\mathbf{T}_2| \geq |\mathbf{T}_1|$, we cannot OR templates of different sizes. Therefore, we will randomly allocate each Bloom filter of the first template ($\mathbf{b}_i^1 \in \mathbf{C}^1$ for $i = 1, \ldots, nBlocks_1$) on the second template, fulfilling two requirements: *i*) there is no overlap in that allocation, and *ii*) we will allocate on average the same number of Bloom filters $\mathbf{b}_i^1 \in \mathbf{C}^1$ over each bigger Bloom filter $\mathbf{b}_j^2 \in \mathbf{C}^2$, with $j = 1, \ldots, nBlocks_2$ (i.e., $nBlocks_1/nBlocks_2$ on average). To that end, we will generate a random vector $\{pos_i\}_{i=1}^{nBlocks_1}$ that will determine where to allocate each Bloom filter $\mathbf{b}_i^1 \in \mathbf{C}^1$. Finally, the OR will be carried out on those parts, keeping the contents of the second template for the remaining bits, which is equivalent to ORing them with the neutral element, 0. In Fig. 5.5 we show an example of such a fusion, where the second and bigger template is depicted in red, the smaller template in blue, and the fused parts are depicted in purple, representing the fusion of the two original red and blue templates.

We further present an improvement with respect to this simple feature level fusion, inspired on weighted score level fusion approaches. Whereas fusing templates at feature level offers a higher security, score level can provide better accuracy when the fused score is computed as a weighted sum: $s = \alpha \cdot s_1 + (1 - \alpha) \cdot s_2$. Therefore, we propose a weighted feature level fusion in which the contribution of each characteristic to the final template can be optimized to maximize, for example, verification accuracy. For a balanced fusion (i.e., assigning equal weights of $\alpha = 0.5$), each characteristic would ideally activate a similar number of bits in the fused Bloom filters. To that end, we need to take into account the average number of bits activated in the final fused template for each characteristic:

- The first characteristic (in blue in Fig. 5.5) activates $|\mathbf{b}_1|$ bits within each individual Bloom filter. Since, on average, $nBlocks_1/nBlocks_2$ filters are mapped into a single fused filter, the final number of activated bits is

$$|\mathbf{b}_1^{fusion}| = |\mathbf{b}_1| \times (nBlocks_1/nBlocks_2) \tag{5.12}$$

- The second characteristic (in red in Fig. 5.5) activates $|\mathbf{b}_2|$ bits in both the individual and the fused templates.

Therefore, in order to reach the desired balance, assuming that $|\mathbf{b}_2| \leq |\mathbf{b}_1^{fusion}|$, the number of bits activated by the second characteristic will be artificially increased applying a Multi-Key XOR (MK-XOR) to each word during the Bloom filter computation. An example for a particular word $\mathbf{w}$ is shown in Fig. 5.5, where $\mathbf{w}$ is XORed with a random set of keys $\mathbf{K} = \{K_1, \ldots, K_{n_\alpha}\}$, hence activating n_α bits instead of just one bit in the Bloom filter $\mathbf{b}$: $\{\mathbf{w} \oplus K_1, \ldots, \mathbf{w} \oplus K_{n_\alpha}\}$. The appropriate number of keys for a balanced fusion, $n_{0.5}$, will be estimated as the ratio between the aforementioned numbers of activated bits:

$$n_{0.5} = \left\lceil \frac{|\mathbf{b}_1^{fusion}|}{|\mathbf{b}_2|} \right\rceil = \left\lceil \frac{|\mathbf{b}_1| \times (nBlocks_1/nBlocks_2)}{|\mathbf{b}_2|} \right\rceil \tag{5.13}$$

Finally to obtain a particular weight α, the corresponding number of keys n_α is estimated as

$$n_\alpha = \left\lceil \frac{\alpha}{0.5} \cdot n_{0.5} \right\rceil = \left\lceil \frac{\alpha}{0.5} \cdot \frac{|\mathbf{b}_1| \times (nBlocks_1/nBlocks_2)}{|\mathbf{b}_2|} \right\rceil \tag{5.14}$$

5.1.4. Potential Attacks

As mentioned in Chapter 3, Sect. 3.2, not only similarity scores have to be analysed during a security and privacy evaluation, but also potential attacks: an eventual attacker may take advantage of certain statistical properties or weaknesses of the template protection scheme. For this reason, the robustness of the proposed improved system needs to be analysed with respect to already proposed as well as foreseeable attacks. To that end, two different adversary models will be considered:

- *Advanced model*: In this model, the adversary has the full knowledge of the algorithms used for template extraction, template protection and comparison, following Kerckhoffs' principles [Kerckhoffs, 1883]. In addition, the adversary is capable of executing part of or all sub-modules of the system that make use of the secret keys, while the adversary knows none of the secrets.

- *Full Disclosure Model*: this model is the advanced model augmented by disclosing the secret keys to the adversary.

Table 5.1 categorizes considered attacks according to the goal of the attack, which can either be breaking irreversibility or unlinkability (cross-matching). It is implied that a successful attack on the irreversibility property of a template protection system also breaks unlinkability, i.e. enables cross-matching.

5.1.4.1. Brute Force Attack

A brute-force cross-matching attack on the original concept of Bloom filter-based template protection has been proposed by Bringer *et al.* [2015]. Let $\mathbf{B}$ be a biometric datum which is protected applying two different secret keys $\mathbf{K}_1$ and $\mathbf{K}_2$ resulting in $\mathbf{C}^1 = PIE(\mathbf{B}, \mathbf{K}_1)$ and $\mathbf{C}^2 = PIE(\mathbf{B}, \mathbf{K}_2)$. Since the indices of the resulting sets of Bloom filters $\mathbf{C}^1 = \{\mathbf{b}^1_1, \mathbf{b}^1_2, \ldots, \mathbf{b}^1_{nBlocks}\}$ and $\mathbf{C}^2 = \{\mathbf{b}^2_1, \mathbf{b}^2_2, \ldots, \mathbf{b}^2_{nBlocks}\}$ are visible to an attacker, the following strategy can be employed to cross-match $\mathbf{C}^1$ and $\mathbf{C}^2$. Each index of one of the two associated Bloom filters is XORed with every possible secret $\mathbf{T}^* \in \{0,1\}^{nBits}$ and it is checked whether $\mathbf{b}^1_i[j] = \mathbf{b}^2_i[j] \oplus \mathbf{T}^*, j = 0, \ldots, 2^{nBits} - 1$, holds for all non-zero indices. This attack can also be applied if $\mathbf{C}^1$ and $\mathbf{C}^2$ are generated from different biometric inputs of the same subject, by searching for a $\mathbf{T}^*$ which yields a minimum dissimilarity score (S_{BF}) between $\mathbf{C}^1$ and $\mathbf{C}^2$. In case binary blocks are large enough, the brute-force search will also succeed if different keys are used for different blocks.

Table 5.1: *Summary of the potential attacks and adversary models: I and U indicate whether attacks can be performed to break the irreversibility and/or the unlinkability property provided by the scheme.*

Attack Type	**Advanced**	**Full Disclosure**
Brute Force	*U*	–
Reconstruction	*I* / *U*	*I* / *U*
Hamming Weight	*U*	–
Exploiting `XOR`	*U*	–

5.1.4.2. Reconstruction Attack

Given a protected template $\mathbf{C}$, the goal of this attack is to reconstruct a biometric datum $\mathbf{B}'$, which is close to the original biometric input $\mathbf{B}$, i.e. the attack can be employed to break irreversibility and unlinkability. Given one Bloom filter $\mathbf{b}$, for each activated index $i = 1, \ldots, |\mathbf{b}|$, the corresponding word $\mathbf{w}_i$ is reconstructed. The entire feature block is reconstructed as one single word repeated *nWords* times, where that word represents the bit-wise average of the $|\mathbf{b}|$ reconstructed words. In other words, in the final feature word $\mathbf{w}$, a given bit is activated iff it was activated at least $|\mathbf{b}|/2$ times. Bringer *et al.* [2015] carried out this attack against the original iris-based scheme proposed in [Rathgeb *et al.*, 2013a] without applying any secret keys. It is shown that, even though the reconstructed iris-codes have not a realistic appearance, the *HD* between them and the original iris-codes is below the threshold set at FMR = 10^{-4}, thus positively matching the original iris-codes and granting access to eventual impostors.

5.1.4.3. Hamming Weights Attack

An efficient cross-matching attack on the original proposal of Bloom filter-based template protection is presented by Hermans *et al.* [2014]. This attack takes advantage of the fact that if W different words appear within one processed binary block, W different bits will be set to one in the corresponding Bloom filter, regardless of the key used in [Rathgeb *et al.*, 2013a] to achieve unlikability: the `XOR` represents a linear mapping, hence forcing no further collisions. Let us assume that one biometric input $\mathbf{B}$ is protected applying two different secret keys $\mathbf{K}_1$ and $\mathbf{K}_2$, resulting in $\mathbf{C}^1 = \mathit{PIE}(\mathbf{B}, \mathbf{K}_1)$ and $\mathbf{C}^2 = \mathit{PIE}(\mathbf{B}, \mathbf{K}_2)$. This means that, regardless of the values of $\mathbf{K}_1$ and $\mathbf{K}_2$, the Hamming Weights (HW) of $\mathbf{C}_1$ and $\mathbf{C}_2$ will be identical, $|\mathbf{C}^1| = |\mathbf{C}^2|$, since $|\mathbf{b}_1^1| = |\mathbf{b}_1^2|, |\mathbf{b}_2^1| = |\mathbf{b}_2^2|, \ldots, |\mathbf{b}_{nBlocks}^1| = |\mathbf{b}_{nBlocks}^2|$. Based on a theoretical analysis for the setting proposed in [Rathgeb *et al.*, 2013a], the authors report that, in the worst case scenario, this trivial cross-matching attack succeeds with a probability of at least 96%. Furthermore, a security analysis on generating false positives and recovery of the secret is presented, both leading to undesirably low attack complexities [Hermans *et al.*, 2014]. While this attack is more efficient compared to a brute force attack, it is not clear if it can be extended to cross-match protected templates generated from different biometric samples $\mathbf{B}_1 \neq \mathbf{B}_2$ of the same instance.

5.1.4.4. Exploiting the XOR-Operation

In the original concept of Bloom filter-based template protection, the application of a XOR operation represents a linear transform, which is applied to each word of each binary block. Let us assume that one biometric sample $\mathbf{B}$ is protected applying two different secret keys $\mathbf{K}_1$ and $\mathbf{K}_2$, resulting in $\mathbf{C}^1$ and $\mathbf{C}^2$, respectively. An attacker can now analyse bit-vectors consisting of the i-th indices of all Bloom filters in $\mathbf{C}^1$ and search for an identical vector in $\mathbf{C}^2$. Since the same secret key is applied to generate all Bloom filters of one protected template, for each vector $(\mathbf{b}_1^1[i], \mathbf{b}_2^1[i], \ldots, \mathbf{b}_{nBlocks}^1[i])$, $i = 0, \ldots, 2^{nBits} - 1$, there will be an identical vector $(\mathbf{b}_1^2[j], \mathbf{b}_2^2[j], \ldots, \mathbf{b}_{nBlocks}^2[j])$, $j = 0, \ldots, 2^{nBits} - 1$. It is important to note that the mapping between all vectors of $\mathbf{C}_1$ and all vectors of $\mathbf{C}_2$ is bijective. In other words, the XOR operation produces a linear shift of indices within Bloom filters which is identical for each block. This fact can be exploited by an attacker to cross-match two protected templates at reduced computational cost, compared to the brute force attack.

Moreover, this attack can be extended to link protected templates generated from different biometric samples $\mathbf{B}_1 \neq \mathbf{B}_2$ of the same instance. In this case, given $\mathbf{C}^1$ and $\mathbf{C}^2$, the attacker would search for corresponding bit vectors exhibiting a minimum HD, thus obtaining a permuted template $\mathbf{C}^{2'}$. The final decision on whether $\mathbf{C}^1$ and $\mathbf{C}^2$ belong to the same subject will be based on the HD between the first and the permuted templates, i.e., $HD(\mathbf{C}^1, \mathbf{C}^{2'})$.

5.2. Experimental Evaluation

In order to evaluate the soundness of the proposed approach, a two-step experimental protocol is followed, where independent databases (described below) are used in order to ensure unbiased results:

- **Development experiments - Parameter estimation**: in the first set of experiments, run over the development databases, *nBits* and *nWords* are estimated following the approach proposed in Sect. 5.1.2. Four different case studies will be taken into account, whose corresponding baseline unprotected systems are described in the cited sections in Chapter 3: face (Sect. 3.3.3), iris (Sect. 3.3.2.1), fingerprint (Sect. 3.3.5.1) and fingervein (Sect. 3.3.4) verification.

- **Test experiments - Privacy and security evaluation**: the evaluation protocol is designed to, on the one hand, confirm the soundness of the parameters estimated on the development experiments, and on the other hand assess to what extent the proposed approaches meet the requirements of template protection systems defined in [ISO/IEC JTC1 SC27 IT Security Techniques, 2011]. Therefore, the protocol in Sect. 3.2 will be followed, comprising four different analyses:

  - **Accuracy analysis**: the first question to analyse is the soundness of the estimated parameters as well as the impact of the proposed improvements on the biometric

accuracy of the system. Therefore, the accuracy variation between the baseline system and the protected system is analysed in the first set of experiments, according to the protocol proposed in Chapter 3, Sect. 3.1, reporting the EERs and FNMR at a fixed FMR.

- **Irreversibility analysis**: once the accuracy has been evaluated, we will focus on the face case study. In the first place, the irreversibility provided by the proposed improved Bloom filter-based template protection system is analysed. To that end, two different aspects will be considered: *i*) the success probability of guessing the correct original template, and *ii*) given a protected template, the probability that the corresponding unprotected template will be reconstructed applying the reconstruction attack. In this last case, the quality of the reconstructed template is estimated by comparing it to the corresponding original binary feature vector in terms of *HD*.

  In the advanced model, attacks on irreversibility also involve guessing the inverse transforms applied during the structure-preserving feature re-arrangement. In order to analyse the irreversibility achieved by the proposed method, the resulting score distributions will be compared to that of random impostors.
- **Unlinkability analysis**: in order to assess whether the improved system meets the unlinkability requirement, the methodology defined in Chapter 3, Sect. 3.2.2 will be used to analyse and compare the original [Gomez-Barrero *et al.*, 2014c] and improved template protection schemes.
- **Robustness to potential attacks**: finally, all proposed cross-matching attacks are applied to the original and improved BTP systems.

In order to obtain unbiased results, experiments are carried out on two independent sets of databases:

- **Development databases**: in the first set of experiments, the parameters of the system (*nBits* and *nWords*) are estimated over the Biosecure DB for iris, face and fingerprint (see Sect. 3.4.6.1). For the fingervein case study, since Biosecure lacked these data, we used the corresponding samples included in the SDMULA-HMT database (see Sect. 3.4.5.2).
- **Test databases**: for the experimental evaluation, we chose widely used benchmarks, to allow an easier comparison with the state-of-the-art: the IIT Delhi Iris Database version 1.0 for iris (Sect. 3.4.3), the Extended M2VTS multimodal Database for face (Sect. 3.4.2), the FVC2002 database for fingerprint (Sect. 3.4.4), and the UTFVP database for fingervein (Sect. 3.4.5.1). In all cases, mated scores are obtained from all possible intra-class comparisons and non-mated scores are computed comparing the first sample of each subject with the second sample of the remaining subjects. For fingerprint and fingervein, in order to avoid misalignment errors, the protocol followed in [Li *et al.*, 2015] will be used, taking into account only the first two samples of each subject.

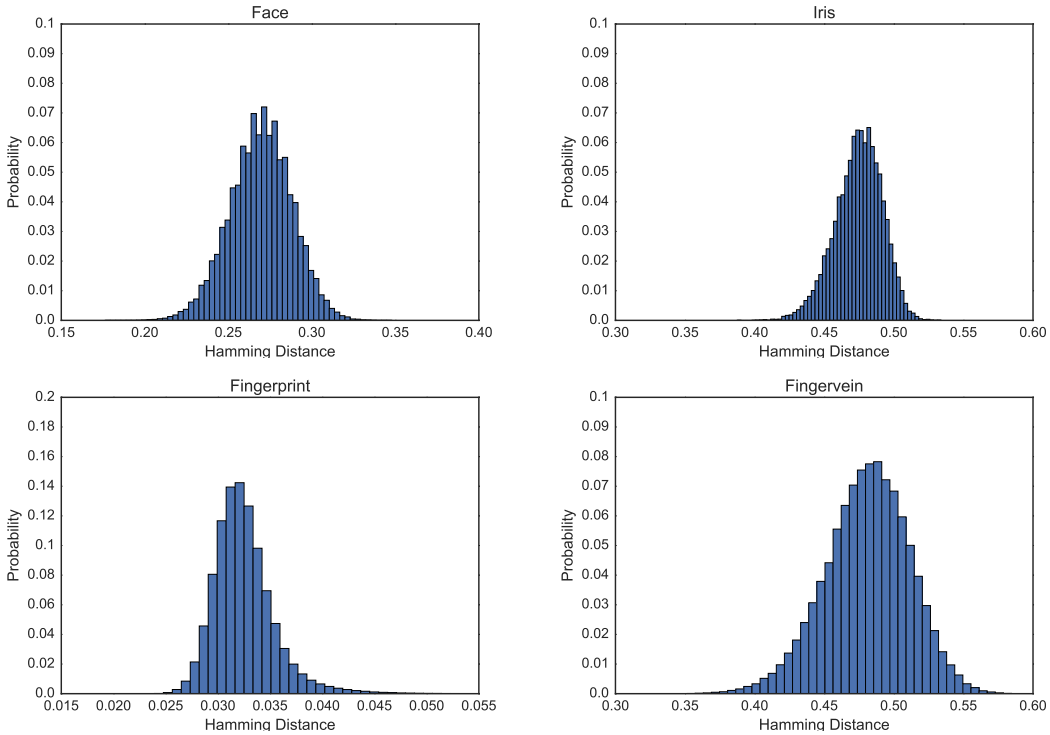


Figure 5.6: *nBits* ***estimation****: distribution of the non-mated Hamming Distances for all the biometric characteristics considered (face, iris, fingerprint and fingervein) on the development databases.*

5.2.1. Parameter Estimation

As described in Sect. 5.1.2, in order to find appropriate values for the two parameters of the system (i.e., *nBits* and *nWords*), we follow a two-step approach: *i*) computation of *nBits* and *ii*) computation of *nWords*.

The *nBits* computation is based on the Degrees of Freedom (N) of the non-mated Hamming distances distributions of the original unprotected templates. Those distribution are depicted for face, iris, fingerprint and fingervein in Fig. 5.6. Then, the upper bound for *nBits* is estimated according to Eq. 5.6. Those bounds and the final value chosen (in parentheses) are presented in Table 5.2 together with the necessary data for Eq. 5.6, namely: mean (p), standard deviation (σ) and N of each distribution, as well as unprotected template sizes $|\mathbf{T}|$. As indicated in Sect. 5.1.2.3, for face templates the computations will be run on the portion of the templates extracted from one sub-image, which comprises 2,400 bits.

As we may observe, the estimated value for face is the lowest one: $nBits = 4$. This is due to the high inter-class variability of face samples, accounting for different lightning conditions, presence or absence of glasses or beards, etc. For iris, an upper bound of 8 is obtained. However, in order to utilize the entire iriscode, comprising 20 rows, we will use $nBits = 10$ as proposed in the original work [Rathgeb *et al.*, 2013a]. For fingerprint, in [Li *et al.*, 2015] a value of $nBits = 13$ was found optimal, very similar to the value found in the present work: $nBits = 12$. Finally, for fingervein an upper bound of $nBits = 9$ was found, which is the value chosen for the following

Table 5.2: *nBits* ***and*** *nWords* ***estimation****. In the first rows, p, σ and N values for the distributions in Fig. 5.6, template sizes |**T**|, and upper bounds for nBits according to Eq. 5.6, with the chosen value in parentheses. In the second set of rows, the estimation of nCols, the corresponding range for nWords and the chosen value in parentheses.*

	Face	Iris	Fingerprint	Fingervein
Mean (p)	0.27	0.47	0.03	0.48
Std (σ)	0.02	0.02	0.003	0.03
DoF (N)	575	623	3,597	269
Template size ($\|\mathbf{T}\|$)	2,400 ($\times$32)	10,240	40,960	4,608
nBits bound (used)	4 (4)	8 (10)	12 (12)	9 (9)
nCols	16	95	186	73
nWords range (used)	[6, 22] (20)	[21, 89] (32)	[41, 174] (53)	[16, 69] (16)

step, since it divides the number of rows of the template, 18. It should be noted that, due to the correlations in both horizontal and vertical directions within the iris and fingervein templates, $N/2$ has been used to estimate *nBits*, as stated in Sect. 5.1.2.1.

In the second step, to give an estimation for *nWords*, we compute the average number of different words in a template for each characteristic, *nCols*. This number is subsequently applied to the inequalities in Eq. 5.10 to estimate the appropriate ranges for *nWords*, setting $R_{min} = 10\%$ and $R_{max} = 45\%$ in order to reach a balance between templates' irreversibility and verification accuracy. Those values, as well as the final ranges, are shown in the second set of rows in Table 5.2. Following the remarks presented in Sect. 5.1.2.2, we have chosen the following values:

- For face, in order to use the whole template extracted from each sub-image, comprising rows of 60 bits, we can choose any of its divisors: $\{6, 10, 12, 15, 20\} \in [6, 22]$. Since the total number of Bloom filters computed is high ($32 \times 40/nBits \times 60/nWords = 19,200/nWords$), we choose $nWords = 20$ in order to maximize the irreversibility.

- For iris, in order to use the whole iriscode (with rows of 512 bits), only powers of 2 will be used: $\{32, 64\} \in [21, 89]$. In order to obtain a sufficient number of Bloom filters and thereby preserve verification accuracy, given that $nBlocks = 20/nBits \times 512/nWords = 1,024/nWords$, we choose $nWords = 32$.

- For fingerprint, in order to have a similar number of Bloom filters as the original approach in [Li *et al.*, 2015], we need to take into account the average number of minutiae vicinities of the templates: $\overline{nVicinities} = 160$. In that approach, the templates extracted from the vicinities were horizontally grouped into three blocks. Therefore, within the estimated range, we choose $nWords = 53 \sim 1/3 \cdot \overline{nVicinities}$, which falls into the computed range, [41, 174].

***Table 5.3: Accuracy Analysis**: EER and FNMR at FMR = 0.01% for the unprotected and protected scenarios considered. For the Bloom filters based schemes, the number of activated bits $|\mathbf{b}|$ is also included.*

		Unimodal Systems			
		Face	Iris	Fingerprint	Fingervein
Unprotected	EER (%)	7.0 ± 0.02	0.6 ± 0.11	1.1 ± 0.67	2.2 ± 0.08
	FNMR (%)	42.3	0.5	1.1	3.3
Protected	EER (%)	4.3 ± 0.02	0.7 ± 0.12	1.2 ± 0.12	3.5 ± 0.01
	FNMR (%)	18.4	0.7	3.9	8.7
	$\lvert\mathbf{b}\rvert$	6.06	22.86	62.64	9.75

		Multimodal: Face + Iris	
		Feature	Score
Unprotected	EER (%)	-	$0.1 \pm 5 \cdot 10^{-5}$
	FNMR (%)	-	0.2
Protected	EER (%)	0.1 ± 0.04	0.3 ± 0.004
	FNMR (%)	0.1	0.5
	$\lvert\mathbf{b}\rvert$	316.07	-

- For fingervein, a range $nWords \in [16, 69]$ is obtained. In order to utilize the whole template, comprising rows of 256 bits, only powers of 2 will be used: $\{16, 32, 64\} \in [16, 69]$. To maintain accuracy a sufficient number of Bloom filters should be computed. As a consequence, given that $nBlocks = 18/nBits \times 256/nWords = 512/nWords$, we choose $nWords = 16$.

It should be noted that for iris and face the ranges comprise the optimal values found in the original approaches [Gomez-Barrero *et al.*, 2014c; Rathgeb *et al.*, 2013a] (i.e., 32 and 20, respectively).

5.2.2. Accuracy Analysis

In order to confirm the soundness of the estimated values for the parameters, we evaluate the accuracy of each unimodal biometric system as well as a multi-biometric system based on face and iris. The Equal Error Rates (EERs), with confidence intervals at 95%, as well as FNMR at FMR = 0.01% are summarised in Table 5.3, while the corresponding Detection Error Trade-off (DET) curves are depicted in Figs. 5.7 and 5.8.

Regarding the unimodal systems, in Fig. 5.7a we may observe that for the face-based system, accuracy is not only preserved for the protected scheme, but even improved (the FNMR is divided by two FMR = 0.01%). On the other hand, since for iris we chose a value for *nBits* slightly higher than the estimated upper bound (ten instead of eight), accuracy could degrade. However,

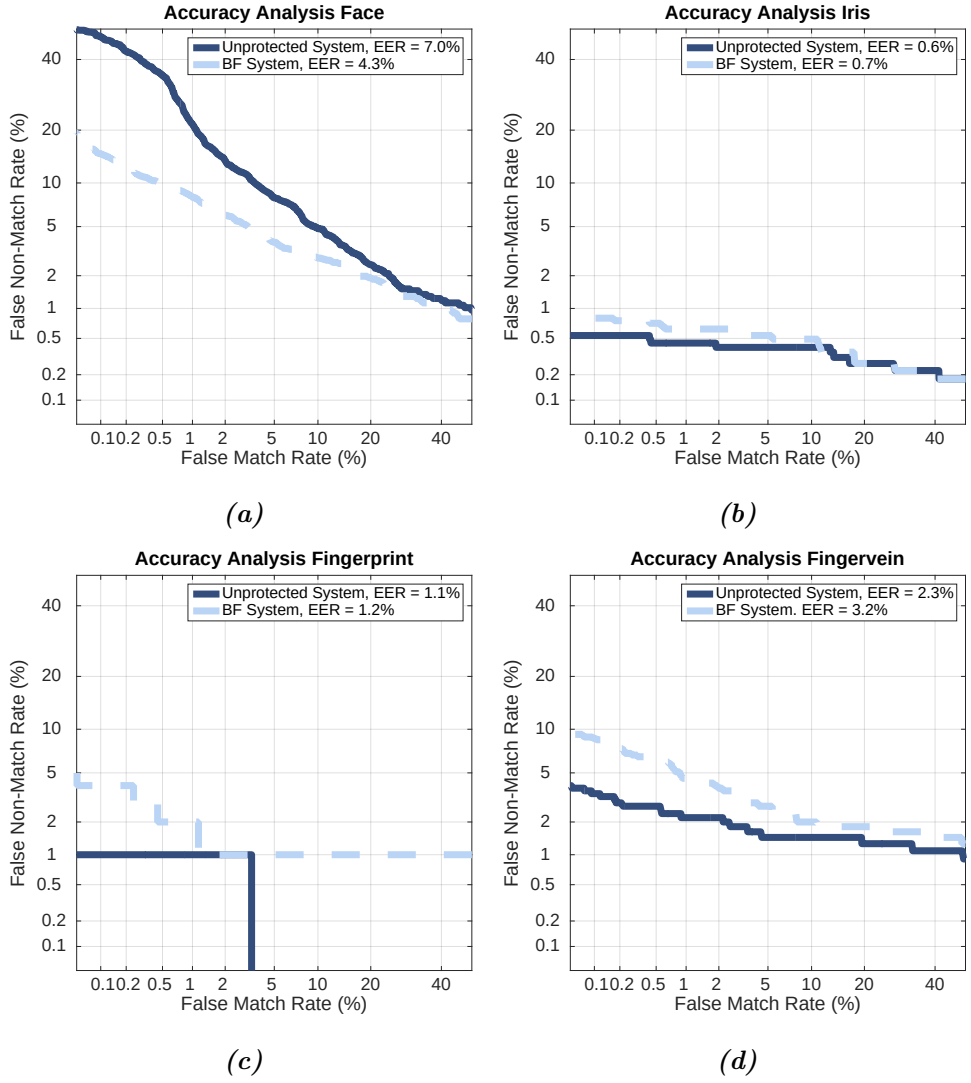
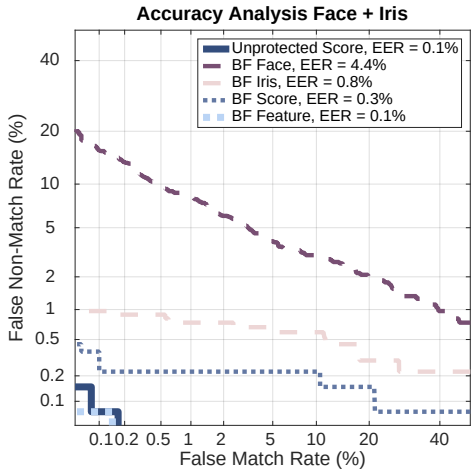


***Figure 5.7: Accuracy analysis**: DET curves for all the biometric characteristics considered, for the unprotected system and the protected BF based scheme using the parameters estimated in Table 5.2. For the multi-biometrc scenario considered (face and iris), fusion is carried out at score level (unprotected and protected) and feature level (protected).*



(a)

Figure 5.8: Accuracy analysis*: DET curves for the multi-biometrc scenario considered (face and iris), where fusion is carried out at score level (unprotected and protected) and feature level (protected).*

taking into account the confidence intervals at 95% confidence, we observe no degradation at the EER. A similar behaviour is observed for fingerprints, thus confirming the soundness of the bounds estimated for *nBits* and *nWords*.

In contrast to the previous case studies, some accuracy degradation is obtained at the EER for fingervein. The reason behind such degradation might be the size of the templates (4,608 bits compared to 76,800 for face, 10,240 for iris or 40,960 for fingerprint), and will be subject to further studies.

It may be observed that, except for the face case study, a stronger degradation in terms of the FNMR is observed for FMR = 0.01% than at the EER. Such increases in the FNMR are due to the intrinsic nature of the Bloom filters, which allow for FMs but not for FNMs. Therefore, a higher FMR could be expected for fixed values of FNMR. Since FNMR is a monotonically decreasing function with respect to FMR, in a similar manner, for a fixed value of FMR a higher value of FNMR could be expected. However, the values provided correspond to high security applications, according to [ANSI-NIST, 2001]. For higher values of FNMR, corresponding to medium security applications, the observed degradation decreases until the EER, where accuracy is preserved.

Once the accuracy variation has been analysed for each unimodal case study, we assess the accuracy of the feature level fusion approach proposed. With the values estimated in the previous section for *nWords* and *nBits*, we first need to estimate and optimize the weight α and its corresponding number of keys n_α for the MK-XOR. According to Eq. 5.13 and Table 5.2, we have

$$n_{0.5} = \left\lceil \frac{6.06 \times (1,024/32)}{22.86} \right\rceil = 9 \tag{5.15}$$

Optimizing the weight α with respect to verification accuracy for values of n_α around nine, we

found an optimal accuracy for $n_{0.7} = 12$.

In order to provide a fair comparison with score level fusions of protected and unprotected templates, we have independently optimized the weights for such fusions, obtaining $\alpha = 0.6$ in the unprotected system, and $\alpha = 0.8$ for the protected score level fusion. As it may be observed, the unprotected score level fusion outperforms the Bloom filter score level fusion. However, the best accuracy, at all operating points, is achieved by the Bloom filter based feature level fusion. Since this fusion is the one providing the highest security and privacy protection, due to the storage of a single template and the further concealment of the biometric data granted with the `OR` operation, we may conclude that the weighted feature level fusion for multi-biometric template protection based on Bloom filters achieves a higher accuracy while further protecting the subject's privacy.

Without loss of generality, and in order to keep the present study within a reasonable length, in the following subsections only the face-based authentication system will be analysed.

5.2.3. Irreversibility Analysis

For the improved face-based template protection scheme, the average number of bits set to one for a given Bloom filter, denoted as $|\overline{\mathbf{b}}|$, and the corresponding average number of remapped words $\overline{R}$, $\overline{R} = 1 - |\overline{\mathbf{b}}|/nWords$, are empirically obtained from the protected templates of all samples in the database. Based on these values, the average number of possible sequences $\overline{nSeq}$ resulting in a single Bloom filter, defined in Eq. 5.4, is raised to *nBlocks*, the number of Bloom filters forming protected templates, in order to estimate the entire inverse image set of the protected template prior to the Bloom filter computation.

Therefore, given a protected template, the success probability of guessing the corresponding unprotected feature vector is estimated as $\overline{nSeq}^{-nBlocks}$ for the full disclosure model, where $\mathbf{K}$ is known to the adversary. In the case of the advanced model, an attacker would further have to guess the employed key $\mathbf{K}$, i.e. the success probability of guessing unprotected feature vectors is calculated as $\overline{nSeq}^{-nBlocks} \times |\mathbf{K}|^{-1}$, which for some configurations is significantly smaller than directly guessing the feature vector of size $nBlocks \times nWords \times nBits = 76,800$. Table 5.4 summarizes the results obtained for the improved system with respect to the level of irreversibility provided, where key space size is estimated as follows, see Eq. 5.5,

$$|\mathbf{K}| = (5 \times 32)!^{32} \approx 2^{30,261} \tag{5.16}$$

It is important to note that those estimations yield lower bounds for success probabilities, since these refer to the probability of guessing the correct original template and not a template which is close to the original one. However, even in case the attacker is in possession of protected templates and their corresponding keys, it is still not possible to directly revert the protected template to the original feature vector. As it may be observed, the success probability of guessing the correct unprotected template is below $2^{-40,000}$ ($\sim 10^{-12,000}$).

Focusing on the reconstruction attack proposed in [Bringer *et al.*, 2015], *HD*-based distributions between the original templates and the ones obtained with the suggested reconstruction

***Table 5.4: Irreversibility analysis**: average number of bits set to one per Bloom filter, average percentage of re-mapped words, average number of possible sequences per block, and success probabilities for guessing original unprotected templates.*

$\lvert\overline{\mathbf{b}}\rvert$	$\overline{R}$ (%)	$\overline{nSeq}$	Success Probability	
			Advanced	Full Disclosure
6.56	56.3	2^{40}	$2^{-71,221}$	$2^{-40,960}$

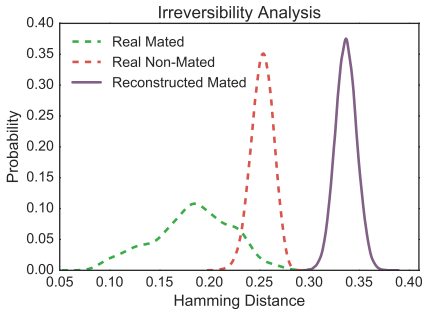


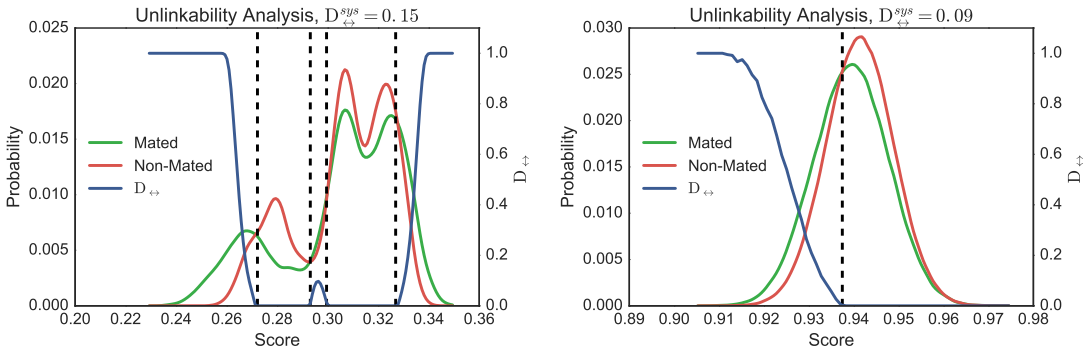
***Figure 5.9: Irreversibility analysis**: HD-based score distributions between the reconstructed and the original unprotected templates, compared to the mated and random non-mated scores between real unprotected templates.*

attack are depicted in Fig. 5.9, where only the full disclosure model has been considered. As can be observed, non-mated *HD*s are even lower than those obtained with the reconstructed templates for the improved system. We conclude that, even for the full disclosure model, the improved system does not allow an efficient reconstruction of templates close to the original ones. Furthermore, yielding *HD*s higher than the random non-mated distances implies that also the security of the system is enhanced, since access will not be granted to such reconstructed templates.

5.2.4. Unlinkability Analysis

In order to assess the level of unlinkability provided by the improved system, we will follow the protocol established in Chapter 3, Sect. 3.2.2. To that end, the two score distributions (i.e., *Mated instances* and *Non-mated instances*) are compared in Fig. 5.10 for sets of $nKeys = 10$ secret keys. $\mathrm{D}_{\leftrightarrow}(s)$ and $\mathrm{D}_{\leftrightarrow}^{sys}$ are also depicted in the same figure.

As it may be observed in Fig. 5.10, the distributions obtained for the improved system (Fig. 5.10b) overlap to a bigger extent than those corresponding to the original system (Fig. 5.10a). In fact, $\mathrm{D}_{\leftrightarrow}^{sys}$ has a small value of 0.09 (67% lower than that of the original system), since only for a small range of scores, $[0.91, 0.94]$, it is slightly more likely that the compared templates represent the same instance. We may thus conclude that templates are almost fully unlinkable when compared in terms of their dissimilarity scores.



(a) *Original system.* ***(b)*** *Improved system.*

Figure 5.10: Unlinkability analysis*: scores distributions for comparisons of protected templates generated with* $nKeys = 10$ *different keys for the original scheme (left) and the improved system (right) The dashed black line represents* $LR(s) = 1$.

5.2.5. Robustness to Cross-Matching Attacks

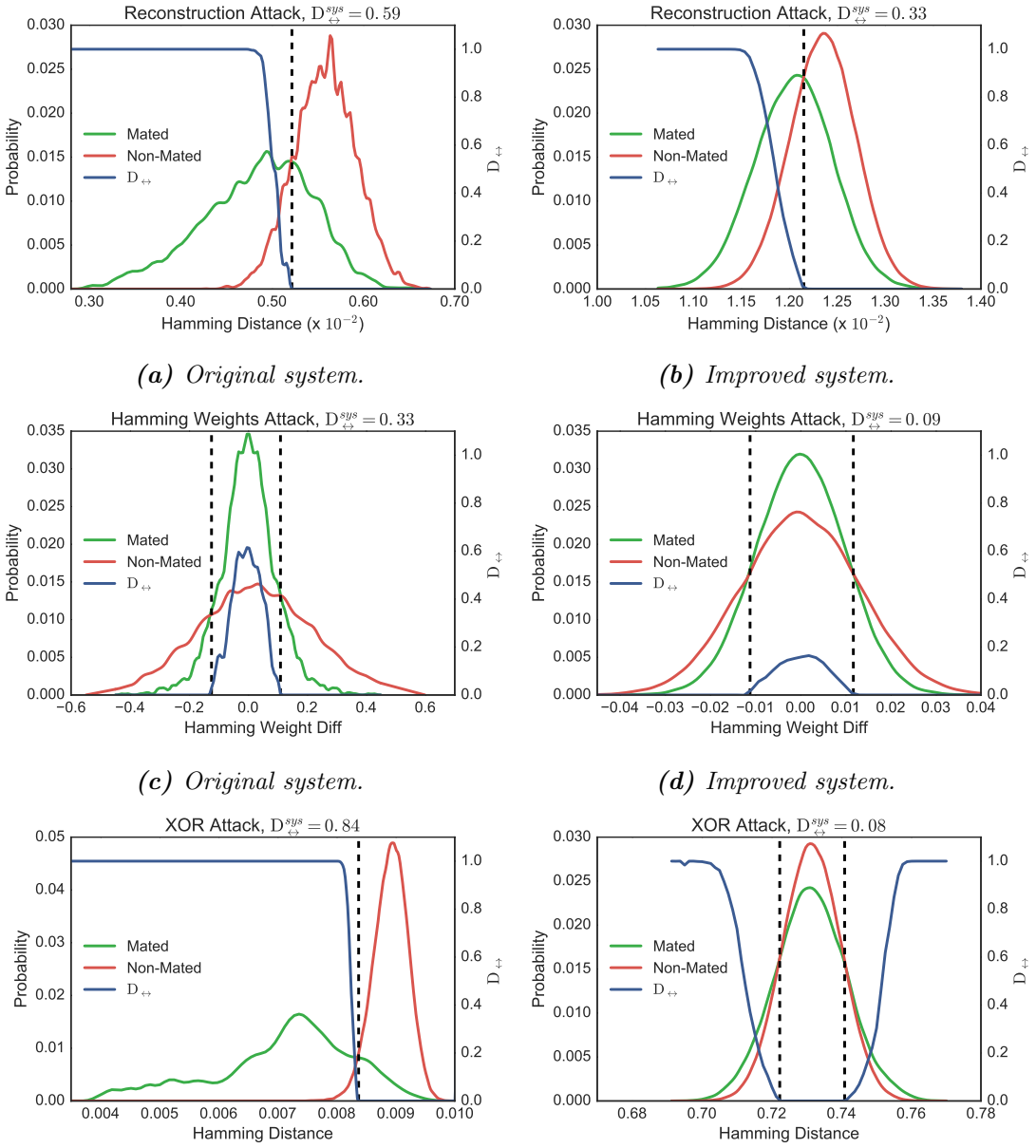
In order to analyse the uniformity of the templates, the entropy of the protected templates is compared to that of the unprotected templates. The entropy, E, is defined as, $E = -\sum p \log p$, where p is the probability of occurrence of a given value. In our particular case, the distribution of bits set to one is first estimated over the whole database, yielding the p probabilities. Then the entropy of those distributions is computed, yielding $E = 4.01$ for feature vectors of the original unprotected system, and $E = 4.08$ for the protected templates. Since the entropy is maintained between both systems, no additional correlations are introduced by the protection scheme and therefore they cannot be exploited by eventual statistical attacks.

Let us now assess the robustness of the enhanced BTP scheme to each of the cross-matching attacks proposed in Sect. 5.1.4.

5.2.5.1. Brute Force Attack

In the advanced model the efficiency of a brute force cross-matching attack depends on the size of the key space: on average, an attacker needs to guess correct sequences of words within feature blocks as well as the key in order to succeed. The average success probability of this attack can be thus estimated as $2(\overline{nSeq}^{-nBlocks} \times |\mathbf{K}|)^{-1}$. Since the suggested structure-preserving feature transforms obscure rows among $nGroups = 32$ groups of binary blocks, the success rate of cross-matching attacks may be increased to $2(\overline{nSeq}^{-nBlocks/nGroups} \times |\mathbf{K}|)^{-1}$, in case the attack is applied simultaneously to each group of blocks. However, even if a brute force cross-matching attack is parallelized for groups of blocks, success rates for the improved system remain rather low. We thus conclude that brute force cross-matching attacks are computationally infeasible.

In the full disclosure model cross-matching would involve guessing the inversion of the Bloom filter-based transform prior to performing the inverse structure-preserving feature re-arrangement, hence, success rates increase to $2(\overline{nSeq}^{-nBlocks})$. For parallelized group-based



(a) *Original system.*

(b) *Improved system.*

(c) *Original system.*

(d) *Improved system.*

(e) *Original system.*

(f) *Improved system.*

Figure 5.11: Robustness to cross-matching attacks*: distributions for the analysis of three different cross-matching attacks for the original scheme (left) and the imrpoved system (right). The dashed black line represents* $LR(s) = 1$.

attacks success rates further increase to $2(\overline{nSeq}^{-nBlocks/nGroups})$, yielding success rates below $2^{-1,279}$. It should be noted that, if block-based transforms such as the `XOR` with one-time pad were applied, success rates would increase to 2^{-39} in case cross-matching is performed simultaneously for each block.

5.2.5.2. Reconstruction Attack

In case of cross-matching, the aim of this attack is to revert two protected templates and link them. Given the low success probabilities estimated for brute force attacks, in this case we restrict the analysis to the full disclosure model. As in the initial unlinkability analysis, the distributions of the *HD*s between the reconstructed unprotected templates generated from the *Mated instances* or *Non-mated instances*, are depicted in Fig. 5.11a and Fig. 5.11b, for the original and improved systems, respectively.

Similar to the unlinkability analysis, the distributions *Mated instances* and *Non-mated instances* overlap to a bigger extent for the improved system, reducing the final $D_{\leftrightarrow}^{sys}$ in 70%, from 0.59 to 0.33. As a consequence, even if the system is more vulnerable to this attack than to the analysis of plain scores under a normal operation mode, for which $D_{\leftrightarrow}^{sys} = 0.09$ (Fig. 5.10b), we may conclude that the templates' robustness to this cross-matching attack has been considerably improved.

In addition, it should be noted that this attack assumes the highest amount of knowledge on the attacker, who is in possession of the secret keys used by the system. Therefore, the $D_{\leftrightarrow}^{sys}$ reaches its highest value for all the cross-matching attacks analysed.

5.2.5.3. Hamming Weights Attack

The *HW*s of the protected templates might be used to cross-match templates generated with different keys. The distributions of the differences in *HW*s between protected templates generated from the *Mated instances* or *Non-mated instances*, are depicted in Fig. 5.11c and Fig. 5.11d, for the original and improved systems, respectively. As we may observe, in both cases all distributions are centred on the same value, zero. However, while for the original system $D_{\leftrightarrow}^{sys} = 0.33$, twice as large as under a normal operation mode (Fig. 5.10a), in the improved system $D_{\leftrightarrow}^{sys} = 0.09$ (i.e., same value obtained for the improved system under normal operational conditions with no attack shown in Fig. 5.10b), reducing the linkability in over 250%. This is due to the fact that for the improved system $D_{\leftrightarrow}(s) < 0.2 \forall s$. Therefore, even for the few cases in which we can assume that two templates belong to the same instance taking into account their *HW*s, the probability of them belonging to different instances is still high, yielding low values of $D_{\leftrightarrow}(s)$. We can hence conclude that templates are robust to this cross-matching attack.

5.2.5.4. Exploiting the XOR-Operation

The XOR operation proposed in the original concept of Bloom filter-based template protection might be exploited to carry out a cross-match attack. To apply this attack, we need to compute *HD*s between optimally re-permuted protected templates. Then, the distributions of such distances, generated from *Mated instances* or *Non-mated instances*, are depicted in Fig. 5.11e and Fig. 5.11f, for the original and improved systems, respectively. As can be observed, the original system is highly vulnerable to this attack: both distributions are easily separable, except for a small range of scores, hence yielding $\mathrm{D}_{\leftrightarrow}^{sys} = 0.84$. On the other hand, for the improved system, only the tails of the *Mated instances* distributions are slightly heavier, thus showing values close to 1 for $\mathrm{D}_{\leftrightarrow}(s)$. This means that the templates yielding those distances are more likely to belong to the same instance. However, since the scores presenting high $D_{\leftrightarrow}(s)$ values (i.e., the distribution tails) are very unlikely to happen, the final unlinkability value achieved for the system is very low, $\mathrm{D}_{\leftrightarrow}^{sys} = 0.08$, which is over ten times smaller than that of the original system, and below the one obtained for the improved system working on normal operation conditions with no attack (see Sect. 5.2.4). Therefore, we may conclude that, unlike the original system, the improved system is robust to cross matching attacks based on the XOR-Operation.

5.3. Chapter Summary and Conclusions

We have proposed in this chapter the first general framework for biometric and multi-biometric template protection based on Bloom filters, where all the information, either stored in the database or handled at verification time, is permanently protected.

An improved version with respect to the system described in [Rathgeb *et al.*, 2013a] has been proposed, in order to meet the unlinkability requirement for protected biometric templates. To that end, an easily integratable module based on a structure-preserving feature re-arrangement of the unprotected templates is added to the original scheme.

Regarding the multi-biometrics approach, the preferred fusion level (i.e., feature level) considered in the ISO/IEC TR 24722 on multimodal and other multi-biometric fusion [ISO/IEC JTC1 SC37 Biometrics, 2007] has been chosen.

According to the protocol established in Chapter 3, Sect. 3.2, we have evaluated the system in order to assess the key requirements within the ISO/IEC IS 24745 on biometric information protection [ISO/IEC JTC1 SC27 IT Security Techniques, 2011], namely: *i*) verification accuracy preservation, *ii*) irreversibility and *iii*) unlinkability. Furthermore, the robustness to potential attacks based on known weaknesses of the original Bloom filter based schemes, has been studied. To that end, experiments were carried out on two sets of widely used and publicly available databases, following a clear protocol in order to make our research reproducible and allow future comparisons to other methods. The main findings of the chapter can be summarised in the following:

- The proposed methodology for the estimation of the key Bloom filter computation param-

eters yields appropriate values, which reach a balance between all requirements proposed in the ISO/IEC IS 24745 on biometric information protection [ISO/IEC JTC1 SC27 IT Security Techniques, 2011].

- In general, there is no accuracy loss in the protected domain. Furthermore, for the proposed multi-biometrics scheme, an EER as low as 0.1% is achieved for the weighted feature level fusion, showing a 85% relative improvement with respect to the best performing individual protected characteristic.
- Only secure irreversible templates are stored in the database or handled at verification time. Furthermore, those references are robust to the reconstruction attack proposed by Bringer *et al.* [2015], hence achieving irreversibility.
- Templates are also unlinkable and robust to already proposed cross-matching attacks [Bringer *et al.*, 2015; Hermans *et al.*, 2014].
- Revocability is achieved with the introduction of the permutation key, thus fulfilling the requirements of the ISO/IEC IS 24745 [ISO/IEC JTC1 SC27 IT Security Techniques, 2011].
- Since no plain information is shared, no biometric information is leaked, thereby preventing inverse biometrics attacks such as the ones presented in Chapter 4.
- The proposed weighted feature-level fusion not only provides the highest security level, requiring the use of a single protected template, but also outperforms the accuracy achieved by a weighted score level fusion.

This chapter includes novel contributions in:

- The proposal of an improved unlinkable and irreversible template protection scheme based on Bloom filters.
- The description of a general framework for the application of Bloom filter based template protection to any given characteristic.
- The proposal of the first template protection scheme for face biometrics based on Bloom filters.
- The proposal of the first template protection scheme for fingervein biometrics based on Bloom filters.
- The proposal of the first multi-biometrics template protection scheme based on Bloom filters based on a weighted feature level fusion, for templates of possibly different sizes.
- The thorough security and privacy evaluation of the aforementioned schemes, taking into account potential cross-matching attacks.

Chapter 6

Biometric Template Protection Based on Homomorphic Encryption

In this chapter we present a generic Biometric and Multi-Biometric Template Protection scheme based on Homomorphic Encryption to deal with the privacy issues unveiled in Chapter 4. Then, we evaluate it in terms of accuracy, irreversibility, unlinkability and computational complexity, in accordance with the security and privacy evaluation protocol established in Chapter 3, Sect. 3.2, and with the requirements established in the ISO/IEC 24745 International Standard on biometric information protection [ISO/IEC JTC1 SC27 IT Security Techniques, 2011].

As indicated in Chapter 2, signal processing in the encrypted domain provides a secure and elegant way to overcome privacy problems [Barni *et al.*, 2015; Lagendijk *et al.*, 2013]. However, its application to biometric recognition systems is still very recent and limited to unimodal fixed-length templates for face, iris or fingerprint.

In this chapter, we present three different systems:

- A scheme based on fixed-length templates, where implementations for computing similarity scores with the Mahalanobis, Euclidean or Cosine distances are given.
- A scheme using variable-length templates and based on the Dynamic Time Warping (DTW) algorithm.
- A multi-biometrics system for feature, score and decision level fusion. In all cases, all computations are carried out in the encrypted domain and only encrypted information is stored or exchanged, in order to avoid any privacy leakage.

It should be also noted that, contrary to the cancelable biometrics approach presented in Chapter 5, in this case the result of the encrypted similarity function is equivalent to that of the unprotected template comparison, whether it is a plain distance measure in the fixed-length templates approach, or the results of a series of distance measurements within the DTW algorithm for the variable-length templates.

According to the security and privacy evaluation methodology described in Chapter 3, Sect. 3.2, the verification accuracy of all the schemes is analysed on a single multimodal and publicly available database, in order to contribute reproducible research and avoid biased results. Furthermore, other desired properties of BTPs, such as irreversibility, unlinkability and computational complexity, are analysed and compared among the cases studies evaluated.

The chapter is structured as follows. Sect. 6.1 gives a brief introduction to Homomorphic Encryption and presents the novel schemes, with one subsection dedicated to each of them: Sect. 6.1.1 describes fixed-length template protection, Sect. 6.1.2 describes variable-length template protection and Sect. 6.1.3 describes multi-biometric template protection. All methods are analysed on Sect. 6.2, in terms of accuracy (Sect. 6.2.1), irreversibility (Sect. 6.2.2) and unlinkability (Sect. 6.2.3), as well as computational complexity (Sect. 6.2.4), for a case study on on-line signature and fingerprint. The chapter summary and conclusions are presented in Sect. 6.3.

This chapter assumes a basic understanding of the fundamentals of pattern recognition [Duda *et al.*, 2001; Theodoridis and Koutroumbas, 2008], image processing [Gonzalez and Woods, 2006], public key cryptography [Ferguson and Schneier, 2003; Goldwasser and Micali, 1984] and Homomorphic Encryption [Fontaine and Galand, 2007].

This chapter is based on the publications: Gomez-Barrero *et al.* [2016a,b,c].

We will use the following notation throughout the Chapter:

- $\mathbf{T}_p = \{p_1, \ldots, p_f, \ldots, p_F\}$ and $\mathbf{T}_r = \{r_1, \ldots, r_f, \ldots, r_F\}$: one-dimensional probe and reference unprotected templates, comprising F features.

- $\mathbf{ST}_p = \{p_1^u, \ldots, p_f^u, \ldots, p_F^u\}_{u=1}^U$: two-dimensional unprotected templates, comprising $F \times U$ features p_f^u. Each F-dimensional point is denoted as $\mathbf{ST}_p[u] = \mathbf{p}^u = \{p_1^u, \ldots, pt_F^u\}$. To simplify notation, to refer to *any* generic point we will use $\mathbf{p} = \{p_1, \ldots, p_F\}$.

- $S_{dist} = d_{dist}(\mathbf{T}_p, \mathbf{T}_r)$: similarity score between two templates $\mathbf{T}_p$ and $\mathbf{T}_r$, where d_{dist} is a particular distance function: *maha* stands for Mahalanobis, *euc* for Euclidean and *cos* for cosine.

- m and m^*: plain message and its corresponding ciphertext.

- $m^* = E_{pk}(m, s)$, where E denotes the encryption function, s a random number and pk the public key, and E is defined in Eq. 6.1. To avoid overcomplicated notation, the encrypted values $E_{pk}(m, s)$ will be simply denoted as $E(m)$, even though the random number s and the public key pk are needed for the encryption computation.

- $m = D_{sk}(m^*)$, where D denotes the decryption function and sk the private key, being D defined in Eq. 6.2.

- $E(\mathbf{T}_r)_{dist}$: encrypted reference template for each distance measure. As will be explained in Sect. 6.1.1, and defined in Eqs. 6.12 and 6.15, the encrypted template $E(\mathbf{T}_r)_{dist}$ is different for each distance. So the reader should be aware that $E(\mathbf{T}_r) \neq \{E(r_1), \ldots, E(r_F)\}$. This

is due to the impossibility to carry out some operations, such as division or square roots, in the encrypted domain. One of the contributions of the Dissertation is defining $E(\mathbf{T}_r)_{dist}$ for each distance measure, so that the score can be directly computed in the encrypted domain.

- $E(S_{dist})$: encrypted similarity score, computed between $\mathbf{T}_p$ and $E(\mathbf{T}_r)_{dist}$ as defined in Eqs. 6.8, 6.11 and 6.14. Following $E(\mathbf{T}_r)_{dist}$, a contribution of the Dissertation is defining, for each of the three considered distance measures, the function $E(S_{dist})$ that takes as input $\mathbf{T}_p$ and $E(\mathbf{T}_r)_{dist}$, and outputs directly the encrypted score with no decryptions involved in the process.

6.1. Biometric Template Protection Based on Homomorphic Encryption

In general, biometric recognition can be performed involving two different entities, as depicted in Fig. 6.1 (left):

- A client, which acquires the probe biometric sample, extracts the features and encodes them in the probe template $\mathbf{T}_p$. Then it generates the similarity score S between the probe $\mathbf{T}_p$ and reference templates $\mathbf{T}_r$, and computes the final mated/non-mated verification decision $D = (S > \delta)$, where δ is the pre-defined verification threshold.

- A server, which holds the database with the reference templates $\mathbf{T}_r$ and sends them to the client during verification.

Such a client-server model might be found, for example, in banking environments, where a central server holds the clients' information, which can be accessed from any local branch.

Due to the issues unveiled in Chapter 4, derived from the use of unprotected templates, the server must process the client's probe biometric data without extracting any information from it, and at the same time, the server must protect the information stored in the database [Barni *et al.*, 2015]. Therefore, in order to increase the privacy of the subject, in the protected system (see Fig. 6.1, right) all the data, either stored or shared between client and either the database or the authentication servers in the verification process, should be encrypted. The database and authentication server should be separate entities in order to avoid information leakage: if encrypted templates were stored with the decryption key, sk, a malicious server or an eventual external attacker could use the secret key to decrypt the templates. As a consequence, we define two different entities and assume that both servers do not collude.

The new roles of the client and the servers are thus the following:

- The client acquires the probe biometric sample, extracts the corresponding template $\mathbf{T}_p$, computes the encrypted similarity score $E(S)$ and sends it to the authentication server.

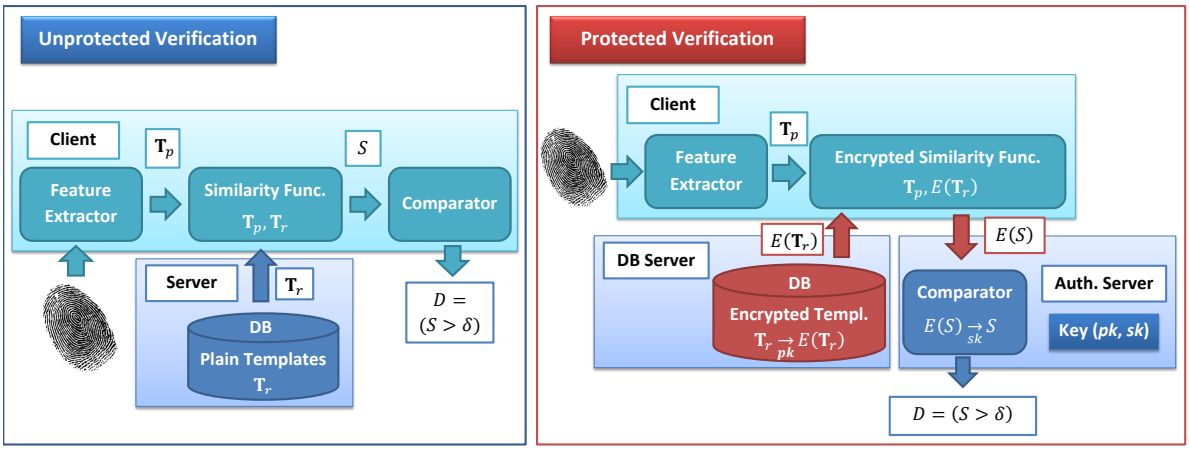


Figure 6.1: Unprotected vs Protected Biometric Verification. *In the unprotected scenario (left), a probe biometric sample is acquired and its features extracted ($\mathbf{T}_p$). The similarity score with respect to the probe reference, $\mathbf{T}_r$, is computed (S). Then, the final output is the mated/non-mated decision, $D = (S > \delta)$. In the protected scenario (right), all the encrypted data or information flow is depicted in red: $E(\mathbf{T}_r)$ and $E(S)$.*

- The DB server holds the database comprising only encrypted templates, and sends the encrypted reference template $E(\mathbf{T}_r)$ to the client during verification.
- The authentication server holds the key pair (pk, sk) and computes the final verification decision D.

As it may be observed, since the client does not know sk, he cannot decrypt the reference template $E(\mathbf{T}_r)$ or the similarity score $E(S)$. This way, the comparator can be moved to the authentication server and S cannot be used to carry out hill-climbing attacks that need access to the score in order to be performed [Galbally *et al.*, 2010b; Gomez-Barrero *et al.*, 2014a; Maiorana *et al.*, 2015]. Furthermore, as it will be shown in Sects. 6.1.1 and 6.1.2, the probe template $\mathbf{T}_p$ does not need to be encrypted, since it never leaves the client. As a consequence there is no leak of biometric information in the communication channel.

In order to encrypt the data, the Paillier homomorphic probabilistic encryption scheme [Paillier, 1999] is used, which is based on the decisional composite residuosity assumption (DCRA): given a composite n and an integer z, it is hard to decide whether z is an n-residue modulo n^2. In other words, it is hard to decided whether there exists y such that $z = y^n \mod n^2$.

As any other public key encryption scheme, two separate keys are required: i) a public key pk for encryption, and ii) a private or secret key sk for decryption. In the Paillier cryptosystem, the public key is defined as $pk = (n, g)$, where $n = p \cdot q$ with p and q two large prime numbers such that $\gcd(pq, (p-1)(q-1)) = 1$, and $g \in \mathbb{Z}^*_{n^2}$. On the other hand, the secret key is defined as $sk = (\lambda, \mu)$, where $\lambda = \text{lcm}(p-1, q-1)$ and $\mu = \left(g^\lambda \mod n^2\right)^{-1} \mod n$.

Given a message $m \in \mathbb{Z}_n$, its encryption is denoted as $m^* = E_{pk}(m, s) \in \mathbb{Z}^*_{n^2}$, and computed as follows:

$$E_{pk}(m, s) = g^m \cdot s^n \mod n^2 \tag{6.1}$$

where $s \in \mathbb{Z}_n^*$ is a random number providing the probabilistic nature of the cryptosystem. This property is necessary to grant semantic security against chosen-plaintext attacks [Goldwasser and Micali, 1984]. In particular, different ciphertexts are obtained when the same plaintext is encrypted several times using the same public key: $E_{pk}(m, s_1) \neq E_{pk}(m, s_2)$. This randomness provides the required unlinkability to the protected templates: even if the exact same unprotected features are extracted from a particular biometric sample, the encrypted templates would be different.

Paillier [1999] showed that E is a one-way function (i.e., irreversible) if and only if the decisional composite residuosity assumption holds. Therefore, a computationally-bound attacker in possession of an encrypted message m^* (a protected biometric template) and the public key pk would not be able to extract any information about the plaintext m (biometric information). He could only do so if he obtained the secret key sk and decrypted the ciphertext $m^* = E_{pk}(m, s)$ as follows

$$m = D_{sk}(m^*) = L\left((m^*)^{\lambda} \mod n^2\right) \cdot \mu \mod n \tag{6.2}$$

where $L(t) = (t-1)/n$.

The main advantage of HE schemes with respect to other cryptosystems is the fact that some operations can be carried out in the encrypted domain, yielding ciphertexts whose corresponding plaintexts are the same we would obtain performing the operations over the plaintexts. In particular, the Paillier cryptosystem fulfils two properties which will be used in the present scheme. On the one hand, the product of two ciphertexts, $m_1^* = E_{pk}(m_1, s_1)$ and $m_2^* = E_{pk}(m_2, s_2)$, will decrypt to the sum of their corresponding plaintexts:

$$D_{sk}\left(m_1^* \cdot m_2^* \mod n^2\right) = m_1 + m_2 \mod n \tag{6.3}$$

On the other hand, an encrypted plaintext, $m_1^* = E_{pk}(m_1, s_1)$, raised to a constant l, will decrypt to the product of the plaintext and the constant:

$$D_{sk}\left((m_1^*)^l \mod n^2\right) = m_1 \cdot l \mod n \tag{6.4}$$

As a consequence, while an unlimited number of summations can be carried out in the encrypted domain, only some products can be computed - as it is shown in Eq. 6.4, one of the factors should be a plaintext. This fact poses a severe challenge for the implementation of many similarity measures or machine learning algorithms.

6.1.1. Fixed-Length Templates

Due to the aforementioned limitation on the operations that can be carried out in the encrypted domain, the main difficulty of designing BTP schemes based on HE lies in the implementation of complex algorithms for the comparison of probe and reference templates. Therefore, an efficient and straightforward approach consists on computing S as the distance between the probe $\mathbf{T}_p$ and the reference template $\mathbf{T}_r$, $S = d(\mathbf{T}_p, \mathbf{T}_r)$ (see Eqs. 6.6, 6.10 and 6.13). Based on this concept, the general diagram of the proposed fixed-length verification system is depicted in Fig. 6.2, where three entities are involved:

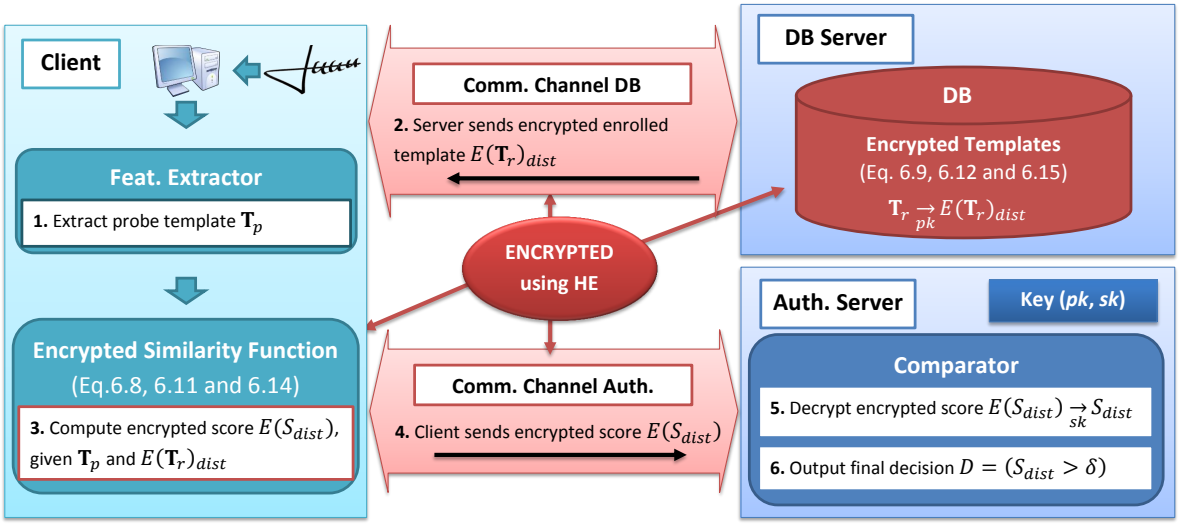


Figure 6.2: General diagram of fixed-length template protection. *A local client acquires and extracts the features of the probe template ($\mathbf{T}_p$) and computes the encrypted dissimilarity score ($E(S)$) between the probe and the reference templates ($\mathbf{T}_r$), according to Eqs. 6.8, 6.11 and 6.14. The DB server holds the encrypted database and the authentication server holds the key pair (pk, sk) and outputs the final decision. All the encrypted values, either stored or transmitted on the communication channel, are depicted in red.*

- The client, which acquires the probe biometric sample, extracts the corresponding template $\mathbf{T}_p$, computes the encrypted similarity score $E(S_{dist})$ and sends it to the authentication server.
- The DB server, which holds the database comprising only encrypted templates, and sends the encrypted reference template $E(\mathbf{T}_r)_{dist}$ to the client during verification.
- The authentication server, which holds the key pair (pk, sk) and computes the final verification decision D.

As it may be observed, identity verification is carried out in six successive steps:

0. During enrolment, the reference biometric templates are encrypted using the server public key pk. The encrypted templates $E(\mathbf{T}_r)_{dist}$ are stored in the database (the encrypted data stored for each distance is explained in the next subsections).
1. The client captures the probe sample and extracts the features, generating the probe template $\mathbf{T}_p$.
2. The DB server sends the reference template $E(\mathbf{T}_r)_{dist}$, encrypted using an HE scheme, to the client.
3. The client computes the encrypted distance between the reference and the probe templates $E(S_{dist})$, given only $\mathbf{T}_p$ and $E(\mathbf{T}_r)_{dist}$ (the implementation of the different distances in

the encrypted domain is explained in the next subsections). It should be noted that one encrypted distance per reference template is computed: $E\left(S_{dist}^{m}\right)$, with $m = 1, \ldots, M$. Then, the product of those scores is considered as the final encrypted similarity score: $E\left(S_{dist}\right) = \prod_{m=1}^{M} E\left(S_{dist}^{m}\right)$, which corresponds to the sum of the scores in the unencrypted domain (see Eq. 6.3).

4. The client sends $E\left(S_{dist}\right)$ to the authentication server.

5. The authentication server decrypts the score, using the secret key sk, thus obtaining S_{dist}.

6. Finally, the authentication server generates and outputs the final genuine/impostor verification decision $D = \left(S_{dist} > \delta\right)$, where δ is a predefined threshold.

It should be noted that, in order to compute $E\left(S_{dist}\right)$, we need to take into account the aforementioned limitations in the operations we can perform in the encrypted domain, and the fact that we can only work with integers. Additionally, all features should be in the same value range in order to carry out the fusion of several characteristics in the multi-biometrics system. To that end, we will consider a two-step approach. First, the real-valued extracted features will be normalized to the interval $[0, 1]$. Then, we will transform those normalized real-valued features to integer values in a bigger range, in our experiments $[0, 10^3]$, in order to retain as much information as possible:

$$X \rightarrow \text{round}\left(10^3 \ X\right) \tag{6.5}$$

6.1.1.1. Encrypted Mahalanobis Distance

Given a user model $\mathbf{T}_r = (\mu, \sigma)$, where $\mu = \{\mu_1, \ldots, \mu_F\}$ and $\sigma = \{\sigma_1^2, \ldots, \sigma_F^2\}$ are the mean and the variance vectors of a set of M stored reference templates, the square Mahalanobis distance of a given template $\mathbf{T}_p = \{p_1, \ldots, p_F\}$ to the model in the encrypted domain is defined as (Fig. 6.1 left)

$$d_{maha}^2\left(\mathbf{T}_p, \mathbf{T}_r\right) = \sum_{f=1}^{F} \frac{\left(p_f - \mu_f\right)^2}{\sigma_f^2} \tag{6.6}$$

Let us see how to compute each addend in the encrypted domain. In order to deal with large enough integers, each of them will be multiplied by 10^6:

$$10^6 \frac{\left(p_f - \mu_f\right)^2}{\sigma_f^2} = 10^6 \left(\frac{p_f^2}{\sigma_f^2} + \frac{\mu_f^2}{\sigma_f^2} - 2\frac{p_f \mu_f}{\sigma_f^2}\right) = p_f^2 \frac{10^6}{\sigma_f^2} + \mu_f^2 \frac{10^6}{\sigma_f^2} - 2 p_f \mu_f \frac{10^6}{\sigma_f^2} \tag{6.7}$$

Applying Eqs. 6.3 and 6.4, the client can compute $E\left(S_{maha}\right)$ as (Fig. 6.1 right)

$$E\left(S_{maha}\right) = \prod_{f=1}^{F} \left\{ E\left(\frac{10^6}{\sigma_f^2}\right)^{p_f^2} \cdot E\left(\mu_f^2 \frac{10^6}{\sigma_f^2}\right) \cdot E\left(\mu_f \frac{10^6}{\sigma_f^2}\right)^{-2p_f} \right\} \tag{6.8}$$

where all three ciphertexts (i.e., encrypted information in Eq. 6.8) are sent by the server, and exponentiations locally computed on the client side. Therefore, we define the reference template

as

$$E\left(\mathbf{T}_r\right)_{maha} = \left\{maha1_f^*, maha2_f^*, maha3_f^*\right\}_{f=1}^{F} \tag{6.9}$$

where $maha1_f^* = E\left(\frac{10^6}{\sigma_f^2}\right)$, $maha2_f^* = E\left(\mu_f^2 \frac{10^6}{\sigma_f^2}\right)$ and $maha3_f^* = E\left(\mu_f \frac{10^6}{\sigma_f^2}\right)$.

In order to be able to encrypt those values, let us now see that $10^6/\sigma_f^2$ is an integer value. By Popoviciu's inequality, given a random variable $X \in [0, c]$, $Var\left(X\right) \leq c^2/4$. Since $p_f \in [0, 10^3]$, we have $\sigma_f^2 = Var\left(p_f\right) \leq 10^6/4 \Leftrightarrow 10^6/\sigma_f^2 \geq 4$.

6.1.1.2. Encrypted Euclidean Distance

Given two F-dimensional templates $\mathbf{T}_p$ and $\mathbf{T}_r$ in the unprotected domain the score $S_{euc} = d_{euc}^2\left(\mathbf{T}_p, \mathbf{T}_r\right)$, can be efficiently computed as (Fig. 6.1 left)

$$S_{euc} = \sum_{f=1}^{F} p_f^2 + r_f^2 - 2p_f r_f \tag{6.10}$$

Then, using Eqs. 6.3 and 6.4, the encrypted score can be directly computed in the encrypted domain without performing any encryptions in the client (Fig. 6.1 right) as

$$E\left(S_{euc}\right) = \prod_{f=1}^{F} E\left(1\right)^{p_f^2} \cdot E\left(r_f^2\right) \cdot E\left(r_f\right)^{-2p_f} = \prod_{f=1}^{F} \left(1^*\right)^{p_f^2} \cdot euc1_f^* \cdot \left(euc2_f^*\right)^{-2p_f} \tag{6.11}$$

The subject's reference template stored in the encrypted database is thus defined by the following ciphertexts:

$$E\left(\mathbf{T}_r\right)_{euc} = \left\{1^*\right\} \cup \left\{euc1_f^*, euc1_f^*\right\}_{f=1}^{F} \tag{6.12}$$

where $euc1_f^* = E\left(r_f^2\right)$ and $euc2_f^* = E\left(r_f\right)$. As a consequence, all cyphertexts involved in Eq. 6.11 are sent by the server, and products and exponentiations locally computed on the client.

It should be noted that, given the probabilistic nature of the Paillier cryptosystem, $E\left(1\right)$ can be computed and stored separately for each subject at enrolment time, leading to different encrypted values and thereby increasing the security and privacy of the subject.

6.1.1.3. Encrypted Cosine Similarity

The cosine similarity between two F-dimensional vectors $\mathbf{T}_p$ and $\mathbf{T}_r$ is defined in the unencrypted domain (Fig. 6.1 left) as

$$d_{cos}\left(\mathbf{T}_p, \mathbf{T}_r\right) = \frac{\mathbf{T}_p \cdot \mathbf{T}_r}{\|\mathbf{T}_p\| \cdot \|\mathbf{T}_r\|} = \sum_{f=1}^{F} \frac{p_f \cdot r_f}{\|\mathbf{T}_p\| \cdot \|\mathbf{T}_r\|} \tag{6.13}$$

Since $d_{cos}\left(\mathbf{T}_p, \mathbf{T}_r\right)$ is a positive number in the range $[0, 1]$, in order to have a bigger range of values that allows a comparison among integers with no significant information loss, we can

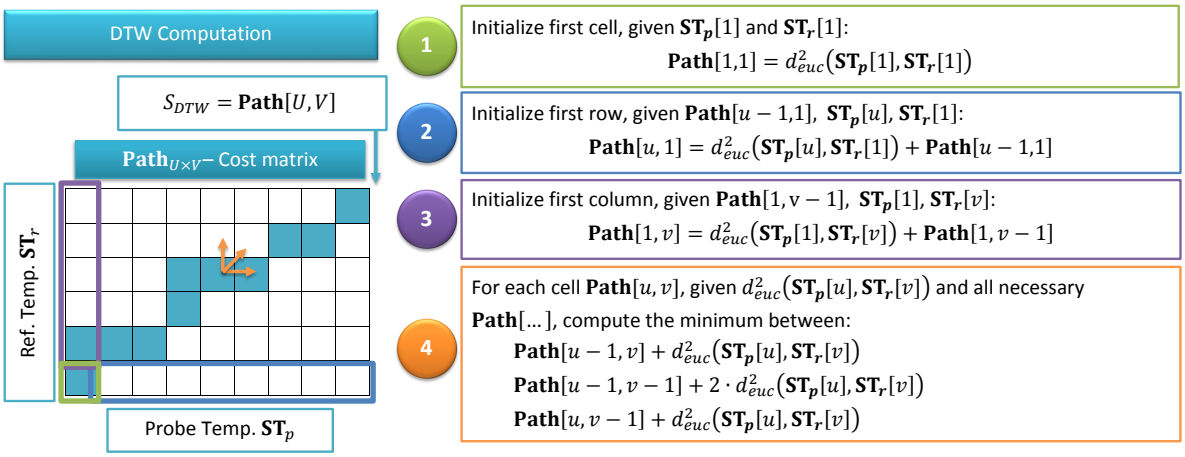


Figure 6.3: Unprotected DTW-based verification. *In order to compare the probe* $\mathbf{ST}_p$ *and the reference* $\mathbf{ST}_r$ *templates, the optimal path, depicted in red, minimizing the Euclidean distance between points, is computed following the DTW algorithm. A cost matrix,* **Path** *is built in four steps. The last entry of the matrix contains the final score* S_{DTW}*.*

compute the final similarity as $S_{cos} = 10^{12} d_{cos}(\mathbf{T}_p, \mathbf{T}_r)$, which can be directly computed in the encrypted domain (Fig. 6.1 right) as

$$E(S_{cos}) = \prod_{f=1}^{F} E\left(\frac{10^6 r_f}{\|\mathbf{T}_r\|}\right)^{10^6 p_f / \|\mathbf{T}_p\|} = \prod_{f=1}^{F} \left(cos_f^*\right)^{10^6 p_f / \|\mathbf{T}_p\|} \tag{6.14}$$

The subject's reference template stored in the encrypted database is therefore defined as

$$E(\mathbf{T}_r)_{cos} = \left\{cos_f^*\right\}_{f=1}^{F} \tag{6.15}$$

where the ciphertexts $cos_f^* = E\left(\frac{10^6 r_f}{\|\mathbf{T}_r\|}\right)$. Therefore, all cyphertexts involved in Eq. 6.14 are sent by the server, and products and exponentiations locally computed on the client.

It should be finally noted that, since $y_f \in [0, 10^3]$, we have $\|\mathbf{T}_r\| = \sqrt{\sum_{f=1}^{F} r_f^2} \leq \sqrt{\sum_{f=1}^{F} 10^6} = 10^3\sqrt{F}$. Therefore, $10^6 r_f / \|\mathbf{T}_r\| \geq 10^6 r_f / 10^3\sqrt{F} = 10^3 r_f / \sqrt{F}$. Assuming $10^3 > \sqrt{F}$, $10^6 r_f / \|\mathbf{T}_r\| \geq r_f$, which yields large enough integers to encrypt.

6.1.2. Variable-Length Templates

In spite of the efficiency of the scheme proposed in the previous section, for some biometric characteristics, such as the signature, better recognition rates are achieved using variable-length templates. To that end, we propose here an implementation within the Paillier cryptosystem of the Dynamic Time Warping (DTW) described in Sect. 3.3.6.1. The baseline unprotected system, in order to obtain a dissimilarity score between the probe ($\mathbf{ST}_p$, of dimensions $U \times F$) and the reference templates ($\mathbf{ST}_r$, of dimensions $V \times F$), computes a cost matrix ($\mathbf{Path}_{U\times V}$), minimizing the distance between signature points in terms of their Euclidean distance. To that end, four steps are carried out (see Fig. 6.3):

1. Initialize first cell:

$$\mathbf{Path}[1,1] = d^2_{euc}\left(\mathbf{ST}_p[1], \mathbf{ST}_r[1]\right)$$

2. Initialize first row:

$$\mathbf{Path}[u,1] = d^2_{euc}\left(\mathbf{ST}_p[u], \mathbf{ST}_r[1]\right) + \mathbf{Path}[u-1,1]$$

3. Initialize first column:

$$\mathbf{Path}[1,v] = d^2_{euc}\left(\mathbf{ST}_p[1], \mathbf{ST}_r[v]\right) + \mathbf{Path}[1,v-1]$$

4. For each of the remaining cells, $\mathbf{Path}[u,v]$ is defined as the minimum between three options:

$$\begin{gathered}\mathbf{Path}[u-1,v-1] + 2 \cdot d^2_{euc}\left(\mathbf{ST}_p[u], \mathbf{ST}_r[v]\right) \\ \mathbf{Path}[u-1,v] + d^2_{euc}\left(\mathbf{ST}_p[u], \mathbf{ST}_r[v]\right) \\ \mathbf{Path}[u,v-1] + d^2_{euc}\left(\mathbf{ST}_p[u], \mathbf{ST}_r[v]\right)\end{gathered}$$

The final dissimilarity score is the last cell of the matrix, namely $S_{DTW} = \mathbf{Path}[U,V]$.

Building upon this unprotected scheme and the approach proposed in [Zhu *et al.*, 2014], a diagram of the encrypted DTW algorithm is shown in Fig. 6.4. As it may be observed, in contrast to its unencrypted version (Fig. 6.3), all computations are now carried out directly in the encrypted domain, yielding an encrypted cost matrix $E\left(\mathbf{Path}_{U\times V}\right)$, obtained from a plain probe template $\mathbf{ST}_p$ and an encrypted reference template $E\left(\mathbf{ST}_r\right)$, where each of the V points are stored as defined in Eq. 6.12. To this end, Eqs. 6.3 and 6.4 are applied to convert steps 1 to 4 to the encrypted domain. This way, summations of plaintexts are substituted by products in the encrypted domain, and products of plaintexts by exponentiations.

The encrypted DTW shown in Fig. 6.4 is used as the matching function of the full verification system depicted in Fig. 6.5. In the complete system, three entities are involved:

- A client, which captures the probe signature sample, extracts the template $\mathbf{ST}_p$, and computes the encrypted cost matrix $E\left(\mathbf{Path}_{U\times V}\right)$ and the encrypted score $E\left(S_{DTW}\right)$ between the probe template and the encrypted reference $E\left(\mathbf{ST}_r\right)$.
- A DB server, which holds the database comprising encrypted templates.
- An authentication server, which collaborates with the client on computing $E\left(S_{DTW}\right)$ and outputs the final binary verification decision $D = (S_{DTW} > \delta)$.

Therefore, two different issues need to be solved in the encrypted domain: *i*) compute the encrypted Euclidean distance between two points $\mathbf{r}$ and $\mathbf{p}$, $E\left(d^2_{euc}\left(\mathbf{r},\mathbf{p}\right)\right)$, having as input $\mathbf{r}$ and $E\left(\mathbf{p}\right)$ (see steps 1 to 4 in Fig. 6.4); and *ii*) compute the minimum between three encrypted values in the $E\left(\mathbf{Path}\right)$ matrix (see step 4 in Fig. 6.4 and steps 4 to 6 in Fig. 6.5). The first issue was already solved in Sect. 6.1.1.2.

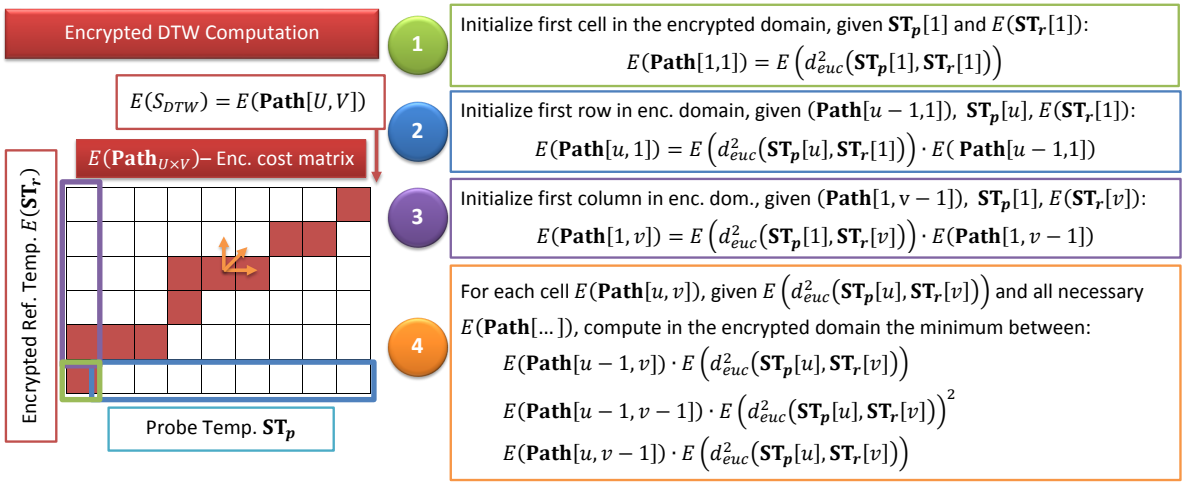


Figure 6.4: Encrypted DTW-based verification. *In order to compare the probe* $\mathbf{ST}_p$ *and the encrypted reference* $E(\mathbf{ST}_r)$ *templates, the encrypted optimal path, depicted in red, minimizing the Euclidean distance between points, is computed following the DTW algorithm depicted in Fig. 6.3. An encrypted cost matrix,* $E(\mathbf{Path})$ *is built in four steps. The last entry of the matrix contains the final score* $E(S_{DTW})$*. It should be noted that all computations are carried out in the encrypted domain.*

In order to compute the minimum between three numbers,

- $a = \mathbf{Path}[u-1, v-1] + 2 \cdot d^2_{euc}(\mathbf{ST}_p[u], \mathbf{ST}_r[v])$,
- $b = \mathbf{Path}[u-1, v] + d^2_{euc}(\mathbf{ST}_p[u], \mathbf{ST}_r[v])$, and
- $c = \mathbf{Path}[u, v-1] + d^2_{euc}(\mathbf{ST}_p[u], \mathbf{ST}_r[v])$

from which only its encrypted values are known to the client, and without revealing any information about the plain values involved to the authentication server, a two-phase protocol is established (Fig. 6.5, steps 4 to 6):

- In step 4, the client generates a list to hide the values to minimize, $E(minList)$. To that end, he computes a set of K random values $N = \{n_{min}, n_2, \ldots, n_K\}$, where $n_k > n_{min}$ for $k = 2, \ldots, K$. Then, the values to be minimized are obscured with n_{min}: $E(m) \rightarrow E(m + n_{min}) = E(m) \cdot E(n_{min})$, with $m = \{a, b, c\}$. To further hide those values, $K-1$ additional numbers are generated randomly choosing one of those original three values, $m_k \in \{a, b, c\}$, and obscuring it with the remaining values in N: $E(m_k) \rightarrow E(m_k) \cdot E(n_k)$, for $k = 2, \ldots, K$. This way, the list comprises:

$$E(minList) = \begin{cases} E(a + n_{min}), E(b + n_{min}), E(c + n_{min}) \\ E(m_k + n_k), \text{with } m_k \in \{a, b, c\}, k = 2, \ldots, K \end{cases} \tag{6.16}$$

- In step 5, the client then sends the complete list $E(minList)$ to the authentication server, who decrypts all the values using its secret key sk, and computes the obscured minimum, $minCost + n_{min}$.

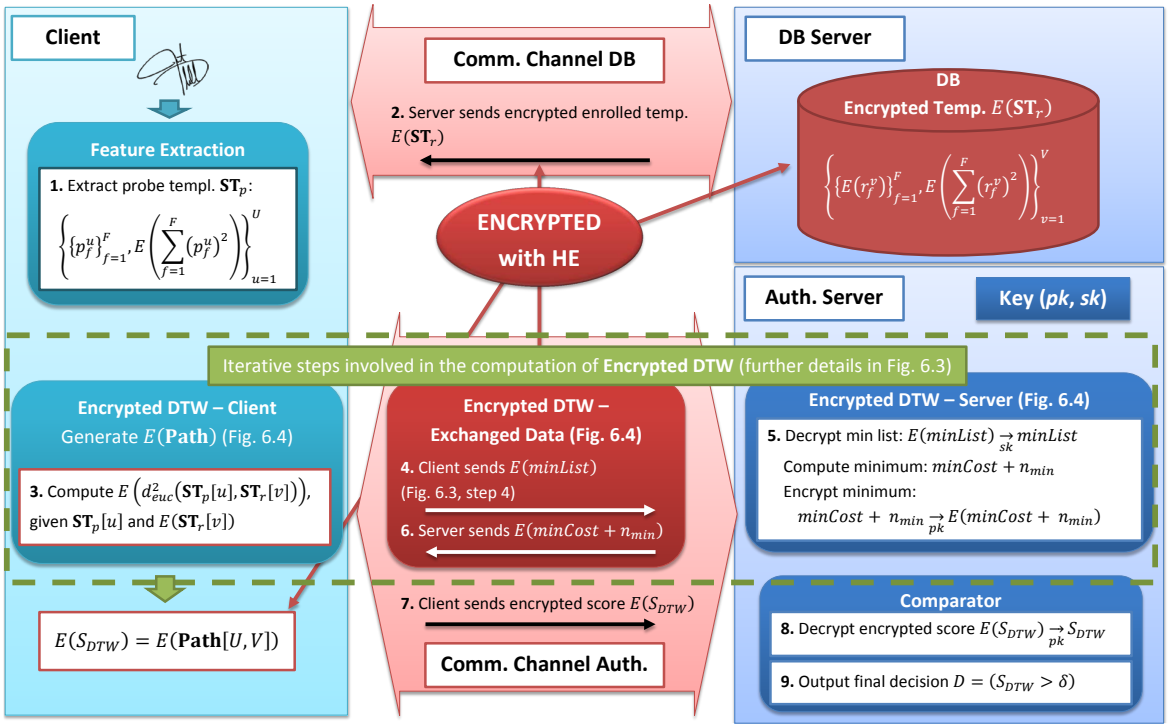


Figure 6.5: General diagram of variable-length template protection. *A local client acquires and extracts the features of the probe sample ($\mathbf{ST}_p$) and computes the encrypted dissimilarity score ($E(S_{DTW})$) between the probe and the reference templates ($\mathbf{ST}_r$), in collaboration with a centralized authentication server. This server holds the key pair (pk, sk) and outputs the final decision. The DB server holds the encrypted database. All the encrypted values, either stored or transmitted, are depicted in red.*

- In step 6, the authentication server sends its encryption back to the client: $E(minCost + n_{min})$.

This way, the client can finally compute $E(minCost) = E(minCost + n_{min}) \cdot E(n_{min})^{-1}$.

Finally the complete verification process is composed of nine steps (see Fig. 6.5):

0. During enrolment, the reference templates $\mathbf{ST}_r$ are acquired, encrypted using the server public key pk to generate $E(\mathbf{ST}_r)_{euc}$ as defined in Eq. 6.12, and stored in the database:

$$E(\mathbf{ST}_r) = \left\{1^*, \{E(r_f^v)\}_{f=1}^F, E\left(\sum_{f=1}^F (r_f^v)^2\right)\right\}_{v=1}^V \tag{6.17}$$

1. The client captures the probe signature sample and extracts the template:

$$\mathbf{ST}_p = \left\{\{p_f^u\}_{f=1}^F\right\}_{u=1}^U \tag{6.18}$$

2. The DB server sends the encrypted reference template $E(\mathbf{ST}_r)$ to the client.

   Steps 3 to 6 are related to the iterative encrypted DTW verification algorithm, depicted inside a green box in Fig. 6.5. In order to obtain the encrypted score, $E(S_{DTW})$, between de probe template, $\mathbf{ST}_p$, and the encrypted reference, $E(\mathbf{ST}_r)$, each value of the encrypted cost matrix $E(\mathbf{Path}[u, v])$ is computed as follows:

3. The client calculates the encrypted Euclidean distance $E\left(d_{euc}^2\left(\mathbf{ST}_p[u], \mathbf{ST}_r[v]\right)\right)$ according to Eq. 6.11.

4. If $u, v \neq 1$ (Fig. 6.4 step 4), the minimum between three values is computed following the two step protocol established above. In this first step, the client generates an encrypted list of values $E\left(minList\right)$ and sends it to the authentication server.

5. The authentication server decrypts the list using sk, finds the obscured minimum $minCost + r_{min}$ and re-encrypts it with pk.

6. The authentication server sends the re-encrypted minimum value to the client, setting $E\left(\mathbf{Path}[u, v]\right) = E\left(minCost\right)$.

7. When the iterative process is finished, the client sends $E\left(S_{DTW}\right) = \mathbf{Path}[U, V]$ to the authentication server.

8. The authentication server decrypts the score with sk, obtaining S_{DTW}.

9. In the last step, the authentication server generates and outputs the final binary verification decision: $D = (S_{DTW} > \delta)$.

6.1.3. Multi-Biometric Template Protection

In order to increase the recognition rates and security provided by BTP schemes, this section builds upon the encrypted distance measures described in Sect. 6.1.1 to present a new HE-based general multi-biometric template protection framework for each fusion level (i.e., feature, score and decision level). In order to avoid overcomplicated notation and with no loss of generality, we will stick to the case of fusing two biometric characteristics: in this particular case study, on-line signature and fingerprint, thus using the superindices fp for fingerprints, sg for signatures and $fused$ for the fusion, where necessary. However, it should be noted that the present framework can be applied to the fusion of any number of characteristics.

6.1.3.1. Feature Level Fusion

At this level, a single protected template comprising all the features, related to both signature and fingerprint, is stored in the database and used at verification time. Therefore, all features are concatenated in a single encrypted template, and a single verification encrypted score $E\left(S\right)$ is computed. Identity verification is thus carried out in six steps, as shown in Fig. 6.6:

0. During enrolment, the reference biometric templates are encrypted using the server public key pk. The encrypted templates $E\left(\mathbf{T}_r^{fp+sg}\right)$ (see Eqs. 6.9, 6.12 and 6.15) are stored in the database.

1. Biometric samples are acquired and a single template, $\mathbf{T}_p^{fp+sg}$, is extracted on the client.

2. The DB server sends the encrypted enrolled template to the client, $E\left(\mathbf{T}_r^{fp+sg}\right)$.

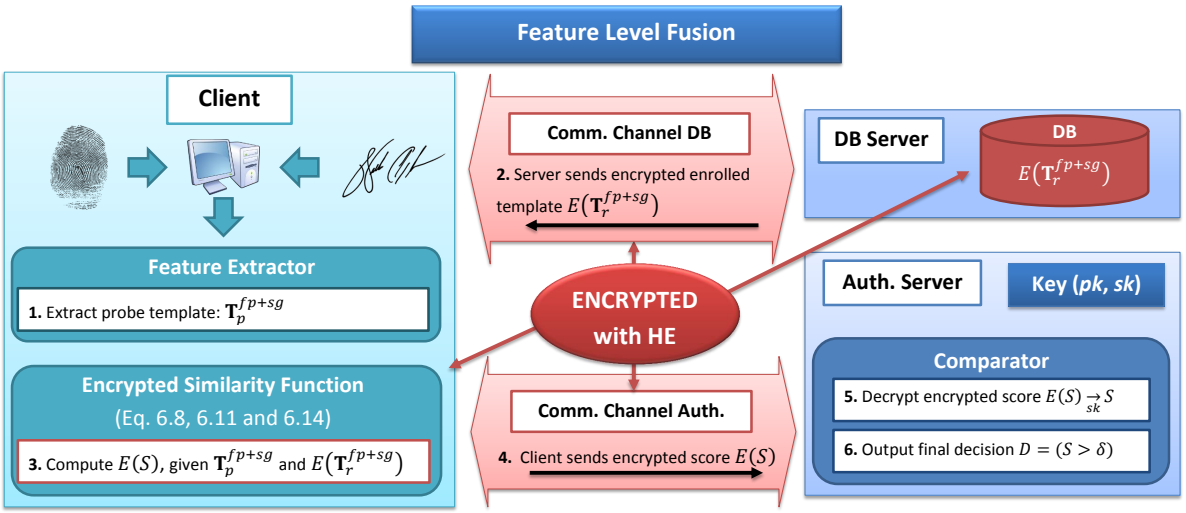


Figure 6.6: General diagram of multi-biometric feature level fusion. *A local client acquires and extracts the features of the probe samples, fusing them into a single template ($\mathbf{T}_p^{fp+sg}$). Then it computes the encrypted dissimilarity score ($E(S)$) between the probe and the reference templates ($\mathbf{T}_r^{fp+sg}$), sending it to a centralized authentication server. This server holds the key pair (pk, sk) and outputs the final decision. The DB server holds the encrypted database. All the encrypted values, either stored or transmitted on the communication channel, are depicted in red.*

3. The client computes the similarity score in the encrypted domain: $E(S)$, according to Eqs. 6.8, 6.11 and 6.14 (depending on the distance measure selected as encrypted similarity function).

4. The encrypted score $E(S)$ is sent to the authentication server.

5. The authentication server decrypts the score using the secret key, sk.

6. Finally, the authentication server compares the score to the verification threshold δ and outputs a mated/non-mated verification decision.

6.1.3.2. Score Level Fusion

In this approach, each biometric characteristic will be processed separately, generating two individual probe templates: $\mathbf{T}_p^{fp}$ and $\mathbf{T}_p^{sg}$. Similarly, the DB server stores and sends $E(\mathbf{T}_r^{fp})$ and $E(\mathbf{T}_r^{sg})$. The client matches them independently to $\mathbf{T}_p^{fp}$ and $\mathbf{T}_p^{sg}$ according to Eqs. 6.8, 6.11 and 6.14, depending on the distance measure considered, producing two individual encrypted scores $E\left(S^{fp}\right)$ and $E\left(S^{sg}\right)$.

In order to normalise the individual scores prior to the fusion, several approaches are proposed in [Jain *et al.*, 2005]. However, it is not possible to implement most of them in the encrypted domain without increasing the computational load due to the restriction in the type of operations that can be performed. We therefore propose a different and simpler approach, that achieves the same accuracy as the min-max rule in the unprotected domain. Since all the scores are

computed with the same distance measure and all the features are normalised to $[0, 10^3]$, for each particular distance the range of variation of the scores will depend on the dimensionality of the templates. Therefore, assuming that the dimensionality of the fingerprint vector is higher $\left(F^{fp} > F^{sg}\right)$, we can perform the following normalisation, which in turn can be easily computed in the encrypted domain:

$$S'^{sg} = \beta S^{sg} \Rightarrow E\left(S'^{sg}\right) = E\left(S^{sg}\right)^{\beta} \tag{6.19}$$

where β is estimated as the average ratio between S^{fp} and S^{sg} for the mated scores.

Then, the final score is computed as the weighted sum of the two partial scores:

$$S = \alpha \cdot \beta \cdot S^{sg} + (10 - \alpha) \cdot S^{fp} \tag{6.20}$$

where $\alpha \in [0, 10]$ and β is the aforementioned normalising parameter.

This way, it follows that the final encrypted score $E\left(S\right)$ can be directly computed from the partial fingerprint and signature encrypted scores, $E\left(S^{fp}\right)$ and $E\left(S^{sg}\right)$, as

$$E\left(S\right) = E(S^{sg})^{\alpha \cdot \beta} \cdot E(S^{fp})^{10-\alpha} \tag{6.21}$$

Seven steps are therefore carried out for verification, as depicted in Fig. 6.7:

0. During enrolment, the reference biometric templates are encrypted using the server public key pk. The encrypted templates $E(\mathbf{T}_r^{fp})$ and $E(\mathbf{T}_r^{sg})$ (see Eqs. 6.9, 6.12 and 6.15) are stored in the database.

1. Biometric samples are acquired and two different templates, $\mathbf{T}_p^{fp}$ and $\mathbf{T}_p^{sg}$, are extracted on the client.

2. The DB server sends the encrypted enrolled templates to the client for each biometric characteristic, $E(\mathbf{T}_r^{fp})$ and $E(\mathbf{T}_r^{sg})$.

3. The client computes in parallel the similarity score for each biometric characteristic in the encrypted domain: $E(S^{fp})$ and $E(S^{sg})$, according to Eqs. 6.8, 6.11 and 6.14 (depending on the distance measure selected as encrypted similarity function).

4. The client fuses the individual scores according to Eq. 6.21.

5. The final encrypted score $E\left(S\right)$ is sent to the authentication server.

6. The authentication server decrypts the score using the secret key, sk.

7. Finally, the authentication server compares the score to the verification threshold δ and outputs a mated/non-mated verification decision.

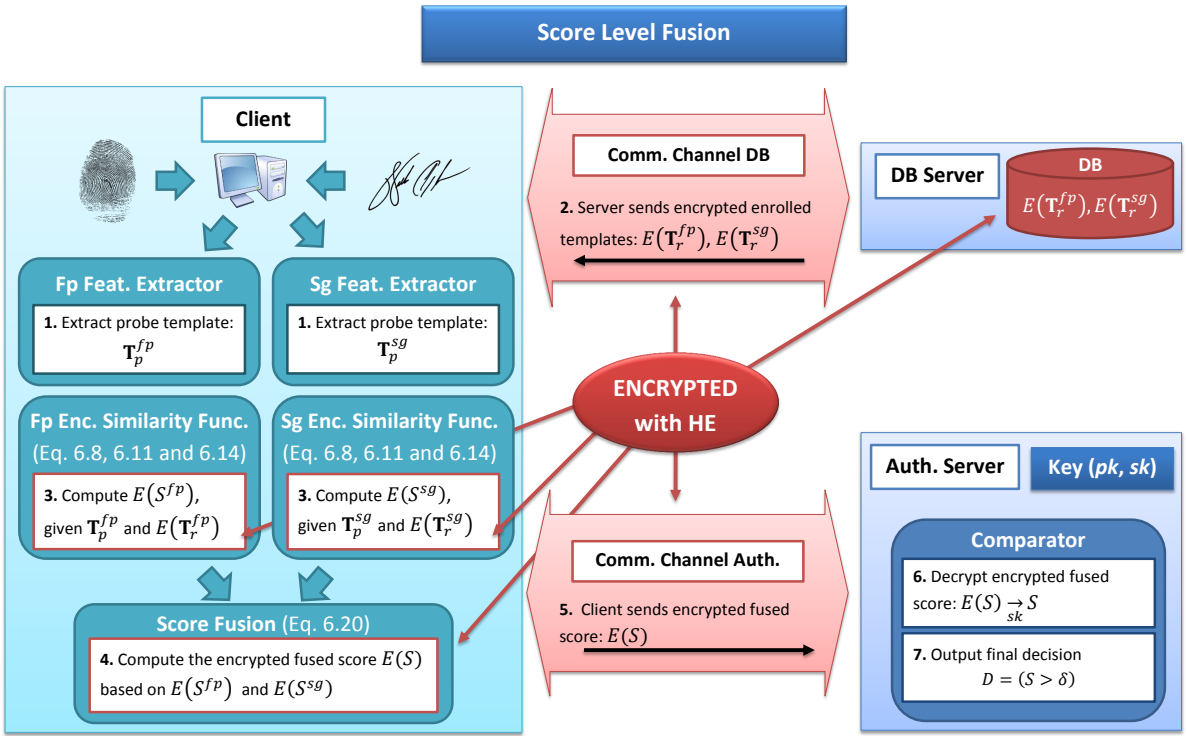


Figure 6.7: General diagram of multi-biometric score level fusion. *A local client acquires and extracts the features of the probe samples, $\mathbf{T}_p^{fp}$ and $\mathbf{T}_p^{fp}$. Then it computes the encrypted dissimilarity scores ($E(S^{fp})$ and $E(S^{sg})$) between the probe and the reference templates ($\mathbf{T}_r^{fp}$ and $\mathbf{T}_r^{sg}$). Finally, both scores are fused into a single score $E(S)$, which is sent to a centralized authentication server. This server holds the key pair (pk, sk) and outputs the final decision. The DB server holds the encrypted templates. All the encrypted values, either stored or transmitted on the communication channel, are depicted in red.*

6.1.3.3. Decision Level Fusion

As in the score level fusion, in this case, each probe biometric sample acquired at the client is processed separately, generating two separate templates: $\mathbf{T}_p^{fp}$ and $\mathbf{T}_p^{sg}$. Both templates are independently compared on the client to $E(\mathbf{T}_r^{fp})$ and $E(\mathbf{T}_r^{sg})$, generating two partial scores $E(S^{fp})$ and $E(S^{sg})$, which are sent to the authentication server. The final binary decision is computed by the server taking into account both partial decisions (D^{sg} and D^{fp}), fused with the `OR` rule:

$$D^{sg} = (S^{sg} > \delta^{sg}) \tag{6.22}$$

$$D^{fp} = (S^{fp} > \delta^{fp}) \tag{6.23}$$

$$D_{\texttt{OR}} = D^{sg} \quad \texttt{OR} \quad D^{fp} \tag{6.24}$$

Although the `OR` rule has been considered in this chapter, as the proposed protection framework is general, any other logic rule could also be used (e.g., `AND`).

As in the previous case, seven steps are carried out during verification (see Fig. 6.8):

0. During enrolment, the reference biometric templates are encrypted using the server public

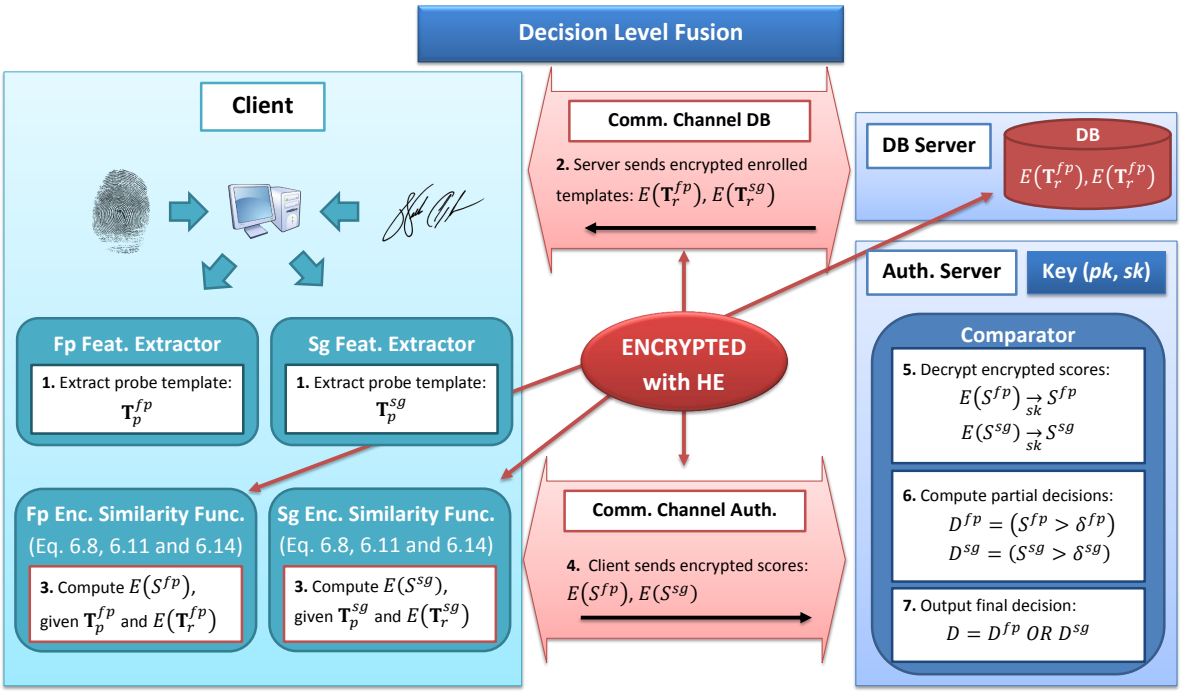


Figure 6.8: General diagram of multi-biometric decision level fusion. *A local client acquires and extracts the features of the probe samples, $\mathbf{T}_p^{fp}$ and $\mathbf{T}_p^{fp}$. Then it computes the encrypted dissimilarity scores ($E\left(S^{fp}\right)$ and $E\left(S^{sg}\right)$) between the probe and the reference templates ($\mathbf{T}_r^{fp}$ and $\mathbf{T}_r^{sg}$), sending them to a centralized server. This server holds the key pair (pk, sk), computes the partial decisions D^{fp} and D^{sg}, fuses them and outputs the final decision. The DB server holds the encrypted templates. All the encrypted values, either stored or transmitted on the communication channel, are depicted in red.*

key pk. The encrypted templates $E(\mathbf{T}_r^{fp})$ and $E(\mathbf{T}_r^{sg})$ (see Eqs. 6.9, 6.12 and 6.15) are stored in the database.

1. Biometric samples are acquired and two different templates, $\mathbf{T}_p^{fp}$ and $\mathbf{T}_p^{sg}$, are extracted on the client.

2. The DB server sends the encrypted enrolled templates to the client for each biometric characteristic, $E(\mathbf{T}_r^{fp})$ and $E(\mathbf{T}_r^{sg})$.

3. The client computes in parallel the similarity score for each biometric characteristic in the encrypted domain: $E(S^{fp})$ and $E(S^{sg})$, according to Eqs. 6.8, 6.11 and 6.14 (depending on the distance measure selected as encrypted similarity function).

4. The individual encrypted scores, $E(S^{fp})$ and $E(S^{sg})$, are sent to the authentication server.

5. The authentication server decrypts both scores using the secret key, sk.

6. Each score is compared to its corresponding threshold (δ^{fp} and δ^{sg}) in order to generate the individual decision, D^{fp} and D^{sg}.

7. Finally, the authentication server fuses the individual D^{fp} and D^{sg} decisions (in this particular case following the `OR` rule) and outputs a mated/non-mated verification decision.

6.2. Experimental Evaluation

Following the methodology described in Chapter 3, Sect. 3.2, for the security and privacy evaluation of biometric systems, an experimental and theoretical analysis will be carried out, involving four key steps:

- **Accuracy analysis**: verification accuracy will be evaluated in Sect. 6.2.1 over the publicly available BiosecurID Multimodal database [Fierrez *et al.*, 2009]. We will compare the accuracy of the biometric and multi-biometric systems, for the unprotected and the protected scenarios.
- **Irreversibility analysis**: given the cryptographic background of the HE algorithm used for the protection of the templates, this property will be theoretically analysed in Sect. 6.2.2.
- **Unlinkability analysis**: similarly, this second property of the protected templates will be theoretically analysed in Sect. 6.2.3.
- **Complexity analysis**: finally, we will study the computational complexity at verification time in Sect. 6.2.4, in terms of the most costly operations (encryptions and decryptions, products and exponentiations at verification time) and the storage requirements.

6.2.1. Accuracy Analysis

In order to establish a fair comparison between biometric and multi-biometric accuracy, we have designed a common protocol for all three scenarios (i.e., on-line signature, fingerprint and multi-biometrics). The database is divided into a train set (first 50 subjects) and a test set (last 350 subjects). The score normalization parameter β and the score fusion parameter α (see Eq. 6.21) are estimated over the train set and accuracy is evaluated over the test set. Regarding the test set, the first 300 subjects are enrolled and modelled with the four samples captured in the first session. The remaining 12 samples of those first 300 individuals are used for computing the mated scores ($12 \times 300 = 3,600$ mated scores). Then, the first sample of the last 50 subjects are compared to each subject model, leading to $50 \times 300 = 15,000$ non-mated scores.

We will first analyse the accuracy of the fixed-length templates, in terms of the Detection Error Trade-off (DET) curves, which are shown in Fig. 6.9. For on-line signature (left), two scenarios are considered: *i*) random forgeries (thick blue lines) and *ii*) skilled forgeries (thin purple lines). Only the former can be analysed for fingerprint (right). For both characteristics, the unprotected system's curves are depicted with solid dark lines, and the protected scheme with bright dashed lines. As it may be observed, the dashed curves (HE protected schemes) and the solid curves (original unprotected systems) completely overlap, except for the Mahalanobis

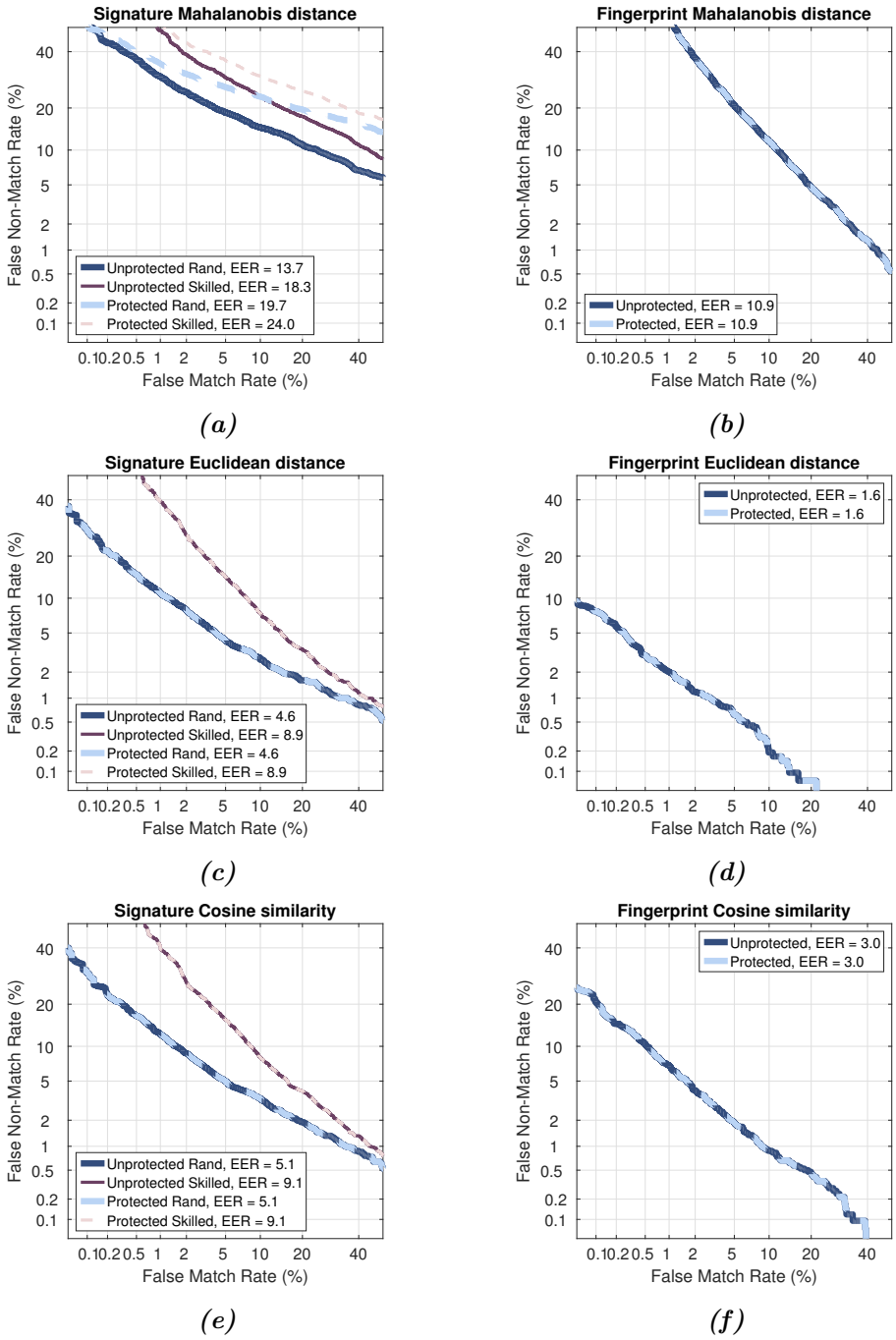


Figure 6.9: Unimodal fixed-length accuracy evalution. *DET curves for the three distances considered, for on-line signature (left) and fingerprint (right), under random (thick blue) and skilled (thin purple) forgeries scenarios, for the original unprotected scheme (solid) and the protected scheme (dashed).*

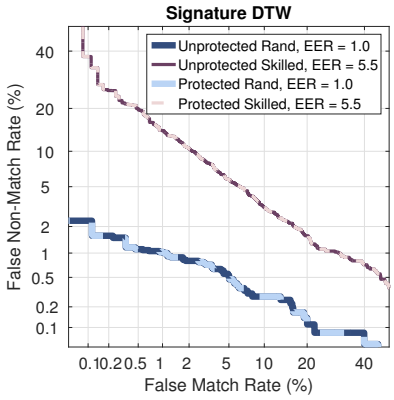
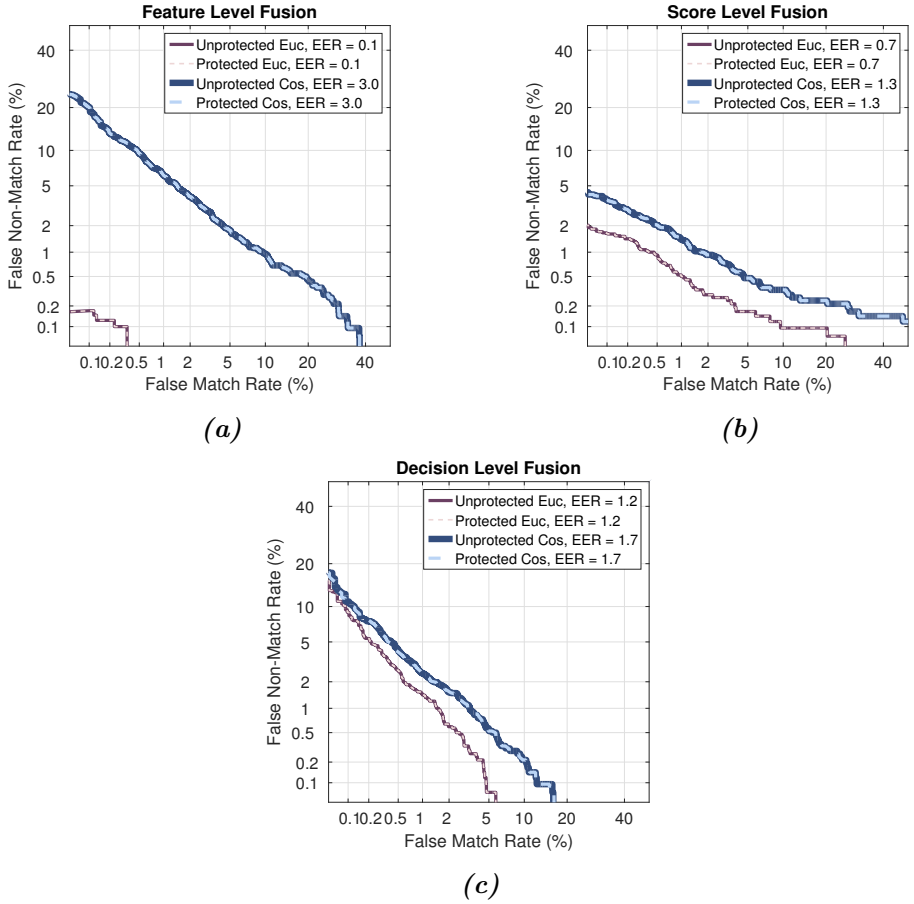


Figure 6.10: Unimodal variable-length accuracy analysis. *DET curves for the three distances considered, for on-line signature under random (thick blue) and skilled (thin purple) forgeries scenarios, for the original unprotected scheme (solid) and the protected scheme (dashed).*



(a) ***(b)*** ***(c)***

Figure 6.11: Multi-biometrics accuracy analysis. *DET curves for the Euclidean (thin purple) and the Cosine similarity (thick blue) for the unprotected (solid) and the protected (dashed) templates, for all the fusion approaches.*

Table 6.1: Accuracy analysis. *EERs for the biometric (only random forgeries scenario) and multi-biometric systems for the unprotected and the protected domains.*

	Mahalanobis		Euclidean		Cosine	
	Unprotected	Protected	Unprotected	Protected	Unprotected	Protected
Signature DTW	-	-	1.0	1.0	-	-
Signature	13.7	19.7	4.6	4.6	5.1	5.1
Fingerprint	10.9	10.9	1.6	1.6	3.0	3.0
Feature	9.3	17.0	0.1	0.2	3.0	3.0
Score	17.0	18.7	0.7	0.7	1.3	1.3
Decision	6.3	7.2	1.2	1.2	1.7	1.7

distance in the on-line signature based system (Fig. 6.9a). In this particular case, accuracy degrades between 44% (random forgeries) and 31% (skilled forgeries) at the Equal Error Rate (EER). This is due to the fact that this is the only distance which takes into account subject models, instead of one-to-one comparisons, thus being more severely affected by the rounding errors introduced by the quantization of the original real-valued features (see Eq. 6.5). Furthermore, while the Cosine and Euclidean distances show a very similar accuracy, the Mahalanobis distance shows a lower accuracy, regardless of the forgeries scenario.

Regarding the variable-length system, whose DET curves are shown in Fig. 6.10, the same behaviour can be observed: the curves completely overlap, hence proving there's no accuracy degradation. Additionally, as it could be expected, the accuracy for on-line signature is considerably increased using variable-length templates: EER decreases from 4.6% and 8.9%, for the Euclidean distance, to 1.0% and 5.5%, for the random and the skilled forgeries scenarios, respectively.

For the multi-biometrics schemes, due to the poor accuracy shown by the Mahalnobis distance (Figs. 6.9a and 6.9b), we restrict the analysis to the Euclidean and Cosine distances. First we need to optimize the parameters α and β (see Eq. 6.21 for the score level fusion) over the train subset, using exhaustive search, in order to obtain the best possible accuracy. Then the accuracy is analysed over the test subset. The DET curves for the three fusion levels are depicted Fig. 6.11, where we can observe that accuracy is preserved in all cases. Furthermore, the feature level fusion offers the highest accuracy with an EER of 0.1%.

Therefore, taking into account all the analyses (EERs are summarised in Table 6.1), two general trends are observed:

- The main take away message of the accuracy analysis is that there is no accuracy loss in the protected domain: for all biometric (based on either fixed-length or variable length templates) and multi-biometric schemes, the Euclidean and Cosine distances are robust to the rounding errors introduced by HE (see Eq. 6.5).

- As a secondary observation, the Euclidean distance performs better in all the fixed-length based schemes considered, specially for the multi-biometric fusion. This is a direct conse-

quence of the accuracy for the unimodal systems, for which it shows a higher accuracy. In particular, for the Euclidean distance the EER decreases 92% at feature level, 53% at score level and 25% at decision level with respect to the best performing unimodal characteristic, the fingerprint (see Table 6.1).

6.2.2. Irreversibility Analysis

For all biometric and multi-biometric schemes, under an honest-but-curious threat model, where both parties, client and server, follow the established protocols but may try to learn additional information about the sample/template on the other side, three different pieces of information should be hidden:

- Only the client can have access to the plain probe biometric data $\mathbf{T}_p$.
- The plain reference templates $\mathbf{T}_r$ should not be seen by the client, being only their encrypted version $E(\mathbf{T}_r)$ stored or exchanged.
- The plain score S should not be transmitted as it can potentially be used to perform hill-climbing or inverse-biometrics attacks, such as the ones proposed in Chapter 4.

For each distance measure considered, the information exchanged from the servers to the client is the encrypted reference template $E(\mathbf{T}_r)_{dist}$. Since only the authentication server knows the decryption key, sk, there is no way for the client or the DB server to learn any information from it, given the semantic security granted by Paillier's cryptosystem against chosen-plaintext attacks [Anderson, 2001]. Conversely, the client sends no information about the acquired probe samples $\mathbf{T}_p$ to any of the servers.

Additionally, in the particular case of the DTW based scheme, a fourth piece of information should be hidden both from the servers and from the client:

- The optimal path $\mathbf{Path}_{U\times V}$.

If the DB server could access this path, with the knowledge of the reference template $\mathbf{ST}_r$, it could reconstruct the probe sample being verified, $\mathbf{ST}_p$, and similarly the client could use $\mathbf{ST}_p$ to guess the reference template $\mathbf{ST}_r$.

Furthermore, in order to avoid information leakage about the optimal path, one additional requirement should be met: given two matrix entries with the same values, their encryption should be different. Otherwise, a malicious attacker could find out identical segments within sequences. Given the probabilistic nature of Paillier's cryptosystem, a given message encrypted twice with the same key will yield different ciphertexts: $E_{pk}(m, s_1) \neq E_{pk}(m, s_2)$. We may therefore conclude that no information can be extracted from identical parts of sequences.

Similarly, in the computation of $E(minCost)$, the server re-encrypts the value of $E(minCost + n_{min})$, thus yielding a different ciphertext from the one the client sent. This way, an eventual man-in-the-middle attack could not learn which is the position within the initial

$E(minList)$ of $E(minCost + n_{min})$, since its value has changed with the re-encryption. In addition, during this minimum computation protocol, the client only shares with the server encrypted distances obscured with random values ($E(\mathbf{Path}[u-1, v-1] + n_{min})$, $E(\mathbf{Path}[u-1, v] + n_{min})$, $E(\mathbf{Path}[u, v-1] + n_{min})$), and padded with additional encrypted values, so that not even the minimum distance $minCost$ is known to the server.

Regarding each multi-biometric fusion level, templates are equally irreversible. However, the complexity level varies: since both score and decision levels require a separate storage of encrypted templates, feature level has been identified as the preferable approach [Kelkboom *et al.*, 2009; Paul and Gavrilova, 2012]. Furthermore, while only one encrypted score is sent from the client to the server for the feature and score levels, decision level fusion in our approach requires the exchange of two different encrypted scores (one per instance), which increases slightly the complexity of the system as shown in the next section.

We may thus conclude that the first requirement established by the ISO/IEC 24745 standard, irreversibility, is met.

6.2.3. Unlinkability Analysis

Let us now see why unlinkability is also granted. On the one hand, since unencrypted distances (i.e., similarity scores) between plaintexts are not preserved in the encrypted domain, given two samples $\mathbf{B}_1$ and $\mathbf{B}_2$ stemming from a given instance, their corresponding protected templates $E(\mathbf{T}_1)$ and $E(\mathbf{T}_2)$, encrypted with the same or different keys, are not related. On the other hand, since the Paillier cryptosystem provides semantic security against chosen-plaintext attacks [Anderson, 2001], given a protected template $E(\mathbf{T}_1)$, no information can be feasibly derived about the original unprotected features $\mathbf{T}_1$. That way, no comparison can be established in the unprotected domain between some kind of information retrieved from the protected templates.

Moreover, since the Paillier cryptosystem is based on probabilistic encryption, the randomness incorporated in the encryption algorithm (see Eq. 6.1) leads to different ciphertexts given a particular message. This means that if $\mathbf{T}_r$ is encrypted twice with the same key, the corresponding ciphertexts could not be matched: $E_{pk}(\mathbf{T}_r, s_1) \neq E_{pk}(\mathbf{T}_r, s_2)$. It should be noted that this property is difficult to achieve in cancelable biometric approaches, such as the one proposed in Chapter 5.

Additionally, as stated in Sect. 6.1, only the server has access to the plain score S, and the only output is a mated/non-mated verification decision. Therefore, attacks based on the evolution of the score for different probe signatures, like the hill-climbing attacks described in [Gomez-Barrero *et al.*, 2014a; Maiorana *et al.*, 2015], or the inverse biometrics methods proposed in Chapter 4, are prevented: they lack the necessary feedback to reconstruct an appropriate template or biometric sample.

Finally, we should bear in mind that, even if templates are irreversible and unlinkable, stolen templates could still be used to impersonate the subject. In that case, a new key pair (sk, pk) would be generated and the entire database could be re-encrypted (i.e., re-secured) without

having to re-acquire any new samples from the enrolled subjects, thereby achieving renewability (as pointed out in Chapter 2, this is not possible with cancelable biometrics approaches).

6.2.4. Computational Complexity Analysis

Finally, the computational cost is estimated in terms of the most complex operations, namely: encryptions, decryptions, products and exponentiations carried out at verification time. The encryption of the reference templates $E(\mathbf{T}_r)$ stored in the database is done during the enrolment, where we can assume that time or speed are not restricted.

It should be noted that, for the estimation of the template size (and exchanged data), the size of the modulo $n = p \cdot q$ has to be taken into account: for a length of $|n|$ bits, ciphertexts will be $2|n|$ bits long. In order to achieve a security comparable to a state-of-the-art RSA, we have chosen a modulo of length $|n| = 1024$ bits [Catalano *et al.*, 2001], thus leading to ciphertexts of 2,048 bits = 0.25 KB. Additionally, $M = 4$ enrolment samples are considered.

6.2.4.1. Fixed-Length Templates and Multi-Biometrics

We should first note that no encryptions or decryptions, which are the most costly operations, are carried out in the local client at verification time for any of the distances or fusion level approaches proposed. On the server, only one (unimodal scheme, feature and score levels) or two (decision level) decryptions are needed to compute the final decision D. This way, fast verification is achieved.

Keeping that remark in mind, let us see some numeric examples in Table 6.2, for the on-line signature unimodal system (Table 6.2a) and for each fusion level (Tables 6.2b to 6.2d), where we considered $F^{sg} = 40$ and $F^{fp} = 100$ features.

As it may be observed in Table 6.2a, the Mahalanobis distance is the most efficient one: templates are 25% to 60% smaller than in any of the other two cases, and the number of products and exponentiations is also the lowest (119 vs 479 or 159, and 80 vs 320 or 160). However, its verification accuracy drops considerably (see Fig. 6.9 left). On the other hand, the Cosine similarity shows no accuracy degradation and it can also be computed twice as efficiently as the Euclidean distance. Therefore, we may conclude that the overall most efficient distance measure is the Cosine similarity.

On the other hand, it should be observed that, even if template sizes are reasonable (in all cases lower than 80 KB for the on-line signature system, and lower than 200.25 KB for the multi-biometric scheme), smaller templates are needed in the unprotected domain, comprising from $|\mathbf{T}^{sg}_{maha}| = 0.04$ KB to $|\mathbf{T}^{fp+sg}_{euc}| = 0.55$ KB. This is due to the fact that, in order to be able to compute the distances in the encrypted domain, up to two or three sets of sequences, instead of just one, need to be stored (see Eqs. 6.9 and 6.12). Additionally, whereas each unprotected feature can be encoded as a 8-bit integer, each ciphertext requires 2,048 bits. Both facts lead to encrypted templates 250 to 750 times bigger than the corresponding unprotected templates.

Now, regarding multi-biometric schemes, since the same amount of encrypted information is

***Table 6.2: Complexity analysis for fixed-length templates**, where $F_{sg} = 40$ and $F_{fp} = 100$.*

***(a)** Unimodal system, for $F = 40$ features..*

	Mahalanobis Dist.	Euclidean Distance	Cosine Similarity
Enc / Dec	0 / 1	0 / 1	0 / 1
Products	119	479	159
Exponentiations	80	320	160
Enc. Temp. size ($\|E(\mathbf{T})\|$)	30 KB	81 KB	40 KB
Temp. size ($\|\mathbf{T}\|$)	0.04 KB	0.16 KB	

***(b)** Feature level fusion.*

	Mahalanobis Dist.	Euclidean Distance	Cosine Similarity
Enc / Dec	0 / 1	0 / 1	0 / 1
Products	419	1,679	559
Exponentiations	280	1,120	560
Enc. Temp. size ($\|E(\mathbf{T})\|$)	105 KB	200.25 KB	140 KB
Temp. size ($\|\mathbf{T}\|$)	0.14 KB	0.55 KB	

***(c)** Score level fusion.*

	Mahalanobis Dist.	Euclidean Distance	Cosine Similarity
Enc / Dec	0 / 1	0 / 1	0 / 1
Products	419	1,679	559
Exponentiations	280	1,120	560
Enc. Temp. size ($\|E(\mathbf{T})\|$)	105 KB	200.25 KB	140 KB
Temp. size ($\|\mathbf{T}\|$)	0.14 KB	0.55 KB	

***(d)** Decision level fusion.*

	Mahalanobis Dist.	Euclidean Distance	Cosine Similarity
Enc / Dec	0 / 2	0 / 2	0 / 2
Products	418	1,678	558
Exponentiations	280	1,120	560
Enc. Temp. size ($\|E(\mathbf{T})\|$)	105 KB	200.25 KB	140 KB
Temp. size ($\|\mathbf{T}\|$)	0.14 KB	0.55 KB	

being stored (in a single template for the feature level fusion, and in two different templates for the score and decision levels), the template size remains unchanged across levels. Furthermore, as the only difference between the fusion levels is the computation of a single score (feature level) or the computation of two separate scores (score and decision levels), which might be fused by the client (score level, see Eq. 6.21) or by the server (decision level), the only difference is the computation of one more product on the client for the feature and score level fusions, and of one more decryption on the server for the decision level. Therefore, whenever it is possible to acquire all the samples at the same location, the feature level is preferred: it shows the best verification accuracy, and it is the most computationally efficient (only one template is stored and only one decryption is needed).

Building upon those observations, a generalized complexity analysis is now shown in Table 6.3 for each distance, for the unimodal and each multi-biometric scenario. Let us know see how to obtain those figures for generic M, F and N (number of instances fused) values. We will first analyse the complexity of the unimodal systems, to develop later the analysis for the multi-biometric scenarios. To that end, we should take into account three considerations:

- In order to verify an identity claim, we need to compute M single distances between the probe and each enrolled template for the Cosine and Euclidean distances:

$$E(S) = E\left(\sum_{j=1}^{M} S^j\right) = \prod_{j=1}^{M} E\left(S^j\right)$$

  where M is the number of enrolled templates. Therefore, the complexity of computing a single distance should be multiplied by M.

- In order to combine those individual scores we need to perform $M-1$ additional products in the encrypted domain.

- Similarly, we need to store M templates for each subject.

For the Mahalanobis distance, in order to compute $E(S_{maha})$ (see Eq. 6.8), for each of the F addends the client computes two exponentiations and two products. Then, all addends are multiple with $F-1$ extra products. This leads to a total number of

$$2F + F - 1 = 3F - 1 \text{ products.}$$
$$2F \text{ exponentiations.}$$

Regarding the template size, $3F$ ciphertexts should be stored at the server (Eq. 6.9). Even if those values could be computed using only two of them, that would increase the number of encryptions and decryptions, being usually better to increase only the storage requirements. In this case, the templates would comprise $3F$ ciphertexts.

The Euclidean distance, $E(S_{euc})$ is computed according to Eq. 6.11. Therefore, each score involves $2F$ exponentiations (2 for each factor) and $3F-1$ products (2 for each factor and $F-1$

to combine all factors) for each of the M enrolled samples. With the additional products for the combination of the partial scores, the final number of operations is

$$M\,(3F-1)+(M-1) = 3M\cdot F - 1 \text{ products.}$$
$$2M\cdot F \text{ exponentiations.}$$

Regarding the template size, the server has to keep in the database $M\cdot(2F+1)$ ciphertexts (Eq. 6.12).

Finally, the encrypted cosine similarity is defined according to Eq. 6.14. The client hence computes F exponentiations (one for each factor) and $F-1$ products to combine all factors. With the additional products for the combination of the partial scores, the final number of operations is

$$M\cdot(F-1)+(M-1) = M\cdot F - 1 \text{ products.}$$
$$M\cdot F \text{ exponentiations.}$$

Regarding the template size, the server has to keep in the database $M\cdot F$ ciphertexts (see Eq. 6.15).

In Table 6.3, the template size is measured in terms of the number of ciphertexts stored. Taking a key length of $|n| = 1,024$, each ciphertext comprises 2,048 bits = 0.25 KB. It is thus enough to divide those figures by four in order to know the corresponding size in KB. For the reason mentioned above (i.e., we need to store twice as many values for the Euclidean distance, and thrice as many values for the Mahalanobus distance, and each number requires 2,048 instead of 8 bits), template sizes are multiplied by 250 to 750 in the encrypted domain. Finally, for both distances, in the unimodal schemes one decryption is carried out in the server in order to decrypt the similarity score and output the final decision $D = (S > \delta)$.

Based on those computations, in the multi-biometrics scenarios, where N instances are fused, we should take into account several observations. First of all, for all fusion scenarios, the template comprises now F_{fused} features instead of F, thus increasing its size accordingly (it depends linearly on F). The only difference between the feature level and the other two fusion levels is the storage as single template or as N separate templates, one for each instance.

Regarding the number of operations, for the feature level fusion, we will perform verification in the same way as in the unimodal case, but the templates handled will now comprise $F_{fused} = F_1 + \cdots + F_N$ features. Since all figures depend linearly on F, we just need to change F by F_{fused}.

At score level, we need to perform all the operations for each individual template. Then, $N-1$ additional products and N exponentiations have to be carried out in order to fuse the scores yielded by each characteristic with their corresponding weights. Therefore, for the Mahalanobis

Table 6.3: Detailed complexity analysis for fixed-length templates. *Number of encryptions / decryptions, and operations carried out during verification, as well as storage requirements, where F denotes the number of features of each characteristic used, N the number of characteristics fused, $F_{fused} = F_1 + \cdots + F_N$, and M the number of samples used at enrollment.*

		Mahalanobis Dist.	Euclidean Distance	Cosine Similarity
Unimodal	Enc / Dec	0 / 1	0 / 1	0 / 1
	Products	$3F - 1$	$3M \cdot F - 1$	$M \cdot F - 1$
	Exponentiations	$2F$	$2M \cdot F$	$M \cdot F$
	Enc. Temp. size ($\lvert E(\mathbf{T}) \rvert$, $\times 0.25$ KB)	$3F$	$2M \cdot F + M$	$M \cdot F$
	Temp. size ($\lvert \mathbf{T} \rvert$, $\times 2^{-10}$ KB)	F	$M \cdot F$	
Feature	Enc / Dec	0 / 1	0 / 1	0 / 1
	Products	$3F_{fused} - 1$	$3M \cdot F_{fused} - 1$	$M \cdot F_{fused} - 1$
	Exponentiations	$2F_{fused}$	$2M \cdot F_{fused}$	$M \cdot F_{fused}$
	Enc. Temp. size ($\lvert E(\mathbf{T}) \rvert$, $\times 0.25$ KB)	$3F_{fused}$	$2M \cdot F_{fused} + M$	$M \cdot F_{fused}$
	Temp. size ($\lvert \mathbf{T} \rvert$, $\times 2^{-10}$ KB)	F_{fused}	$M \cdot F_{fused}$	
Score	Enc / Dec	0 / 1	0 / 1	0 / 1
	Products	$3F_{fused} - 1$	$3M \cdot F_{fused} - 1$	$M \cdot F_{fused} - 1$
	Exponentiations	$2F_{fused} + N$	$2M \cdot F_{fused} + N$	$M \cdot F_{fused} + N$
	Enc. Temp. size ($\lvert E(\mathbf{T}) \rvert$, $\times 0.25$ KB)	$3F_{fused}$	$2M \cdot F_{fused} + M$	$M \cdot F_{fused}$
	Temp. size ($\lvert \mathbf{T} \rvert$, $\times 2^{-10}$ KB)	F_{fused}	$M \cdot F_{fused}$	
Decision	Enc / Dec	0 / N	0 / N	0 / N
	Products	$3F_{fused} - 2$	$3M \cdot F_{fused} - N$	$M \cdot F_{fused} - N$
	Exponentiations	$2F_{fused}$	$2M \cdot F_{fused}$	$M \cdot F_{fused}$
	Enc. Temp. size ($\lvert E(\mathbf{T}) \rvert$, $\times 0.25$ KB)	$3F_{fused}$	$2M \cdot F_{fused} + M$	$M \cdot F_{fused}$
	Temp. size ($\lvert \mathbf{T} \rvert$, $\times 2^{-10}$ KB)	F_{fused}	$M \cdot F_{fused}$	

distance the number of operations is

$$\begin{aligned}(3F_1 - 1) + \cdots + (3F_N - 1) + (N - 1) &= (3 \cdot F_{fused} - N) + (N - 1) \\ &= 3F_{fused} - 1 \text{ products.} \\ 2F_1 + \ldots + 2F_N + N &= 2F_{fused} + N \text{ exponentiations.}\end{aligned}$$

Now, for the Euclidean distance the number of operations is

$$\begin{aligned}(3M \cdot F_1 - 1) + \cdots + (3M \cdot F_N - 1) + (N - 1) &= (3M \cdot F_{fused} - N) + (N - 1) \\ &= 3M \cdot F_{fused} - 1 \text{ products.} \\ (2M \cdot F_1) + \ldots + (2M \cdot F_N) + N &= 2M \cdot F_{fused} + N \text{ exponentiations.}\end{aligned}$$

And finally, for the cosine similarity we compute:

$$\begin{aligned}(M \cdot F_1 - 1) + \cdots + (M \cdot F_N - 1) + (N - 1) &= (M \cdot F_{fused} - N) + (N - 1) \\ &= M \cdot F_{fused} - 1 \text{ products.} \\ (M \cdot F_1) + \ldots + (M \cdot F_N) + N &= M \cdot F_{fused} + N \text{ exponentiations.}\end{aligned}$$

At decision level, we need to carry out all the operations for each individual template. Since both products and exponentiations depend linearly on F, we only need to substitute F by F_{fused}. Additionally, since N separate partial similarity scores $E(S_1), \ldots, E(S_N)$ are sent from the client to the server, N instead of one decryptions need to be performed on the server in order to output the D verification decision.

It should be finally noted that in most biometric systems, the number of enrolled samples, M, or fused characteristic, N, are low, in most cases lower than ten. Therefore, since $M, N \ll F$, the number of products and exponentiations increases linearly with F_{fused}, for all fusion levels and distances, achieving a linear complexity of $\mathcal{O}(F_{fused})$.

6.2.4.2. Variable-Length Templates

Let us now analyse the complexity of the DTW based protected verification, starting with some numeric values as in the previous section. For the particular system here proposed, $F = 9$ time sequences and $M = 4$ enrolment samples are used, $K = 10$ random values added in step 4 in Fig. 6.3 to the three values to minimize, and the average sequence length in BiosecurID is $\bar{U} = 370$. Using Kun Liu's implementation of the Paillier cryptosystem in Java[1], and running the experiments in a machine with an Intel Core i7 with four 2.67 GHz cores, one comparison takes approximately two minutes and 450 MB of data are exchanged. It should be noted that this is just an illustrative approximation: code should be optimized and a server, instead of a regular desktop computer, would bear the highest computational cost. Furthermore, a high accuracy is achieved with DTW using a lower number of enrolment samples, thereby reducing the time needed and the amount of exchanged data - in the present chapter we used four in order to allow a fair comparison with the fixed-length templates schemes.

Now, we analyse in detail the complexity in terms of any given F, M and K. First, in Fig. 6.5 step 1, the client extracts the probe template. Then, the server sends to the client the encrypted reference template $E(\mathbf{ST}_r)$, comprising $V \cdot (2M \cdot F + M)$ ciphertexts (see Table 6.3, unimodal Euclidean distance). In order to compute the encrypted cost matrix, it should be noted that no additional encryptions or decryptions are needed for the encrypted distances calculations, since all values had been already encrypted at enrolment. On the other hand, for each of the $(U-1)\cdot(V-1)$ iterations involving a minimum computation (Fig. 6.4, step 4), the client needs to encrypt each of the K random values n_k and send an encrypted list comprising $K+2$ values to the server. The server, in turn, needs to perform $K+2$ decryptions, one encryption, and send one ciphertext back (Fig. 6.5 step 4–6).

[1]Publicly available at http://www.csee.umbc.edu/~kunliu1/research/Paillier.html

Table 6.4: Complexity analysis for variable-length templates.

	Client	Server
Encryptions	$\mathcal{O}\left(U^2K\right)$	$\mathcal{O}\left(U^2\right)$
Decryptions	0	$\mathcal{O}\left(U^2K\right)$
Comm. channel	$\mathcal{O}\left(U^2K\right)$	

To sum up, the client needs to encrypt $(U-1)\cdot(V-1)\cdot K = \mathcal{O}(UVK)$ ciphertexts. The server, on the other hand, decrypts $(U-1)\cdot(V-1)\cdot(K+2) = \mathcal{O}(UVK)$ ciphertexts and encrypts $(U-1)\cdot(V-1) = \mathcal{O}(UV)$ ciphertexts. Finally, $V\cdot(2M\cdot F+M)+(U-1)\cdot(V-1)(K+3) = \mathcal{O}(MFV+UVK) = \mathcal{O}(UVK)$ ciphertexts are exchanged between server and client ($MF \ll UK$). These results are summarized in Table 6.4, where, without loss of generality, UV has been substituted by U^2.

6.3. Chapter Summary and Conclusions

We have proposed in this chapter the first general framework for variable-length and fixed-length, biometric and multi-biometric template protection based on Homomorphic Encryption, where all the information, either stored in the database or exchanged between the client (issuing the identity claim) and the server (holding the database and verifying the identity claim), is encrypted.

Regarding the multi-biometrics approach, different models have been described and analysed for the three fusion levels considered in the ISO/IEC TR 24722 on multimodal and other multi-biometric fusion [ISO/IEC JTC1 SC37 Biometrics, 2007], namely: feature, score and decision level.

According to the protocol established in Chapter 3, we have evaluated the system in order to assess the key requirements within the ISO/IEC IS 24745 on biometric information protection [ISO/IEC JTC1 SC27 IT Security Techniques, 2011], namely: *i*) verification accuracy preservation, *ii*) irreversibility and *iii*) unlinkability. To that end, experiments were carried out on the on-line signature and fingerprint subcorpora of the publicly available BiosecurID multimodal database, following a clear protocol in order to make our research reproducible and allow future comparisons to other methods. The main findings of the chapter can be summarised in the following:

- There is no accuracy loss in the protected domain, regardless of the considered approach. Furthermore, for the proposed multi-biometrics scheme, an EER as low as 0.1% is achieved for the feature level fusion, showing a 92% relative improvement with respect to the best performing individual characteristic. We may therefore conclude that the loss on accuracy due to the use of baseline systems with higher error rates than the current state-of-the-art can be partly compensated fusing two characteristics.

- Only secure irreversible templates are stored in the server's database, hence achieving irreversibility.
- Templates are also unlinkable and renewability is achieved, thus fulfilling the requirements of the ISO/IEC IS 24745 [ISO/IEC JTC1 SC27 IT Security Techniques, 2011].
- Since no plain information is shared, no biometric information is leaked, thereby preventing hill-climbing [Gomez-Barrero *et al.*, 2014a; Maiorana *et al.*, 2015] or inverse biometrics attacks such as the ones presented in Chapter 4.
- While variable-length templates can achieve a better accuracy for characteristics such as on-line signature, they also entail a higher computational load. The proposed scheme based on fixed-length templates can be deployed for real-time applications: no encryptions and only one decryption are performed on the server at verification time, and templates require at most 200 KB, a reasonable size even if is still a high compared to the 0.55 KB in the unprotected domain.
- Feature level fusion is preferable to the other two levels, since it achieves a better accuracy and a unique template is generated for each subject.
- On the other hand, score level fusion is more flexible: it can be implemented in a distributed manner, where each client extracts one biometric sample and computes the corresponding similarity score. In that case, the score fusion would be carried out by the server, without each client having access to the other clients' scores.

In contrast to the aforementioned advantages, using Homomorphic Encryption for biometric template protection entails some limitations. For instance, the implementation of more sophisticated recognition schemes usually implies a higher computational load, or pre-aligned samples may be required.

This chapter includes novel contributions in:

- The implementation of three different distance measure in the encrypted domain, which involves the definition of the encrypted template and the encrypted distance function for each measure, so that the score can be directly computed in the encrypted domain.
- The description of the first variable-length biometric template protection scheme based on Homomorphic Encryption.
- The proposal of the first multi-biometrics template protection scheme based on Homomorphic Encryption for feature, score and decision level fusion.
- The experimental analysis of the accuracy variation on a real multimodal database.
- The unlinkability, irreversibility and computational load analysis of the protected templates.

Chapter 7

Conclusions and Future Work

This Thesis has considered the problem of evaluating the security and privacy provided by biometric systems, through a systematic analysis of the accuracy of the systems, as well as the irreversibility and unlinkability of the templates. After a summary of the state-of-the-art in inverse biometrics and biometric template protection, the security and privacy evaluation methodology followed in the Thesis has been presented. In particular, a new framework for the systematic analysis of templates unlinkability has been proposed. Furthermore, novel methods for inverse biometrics and template protection, for both biometric and multi-biometric systems have been developed. The procedural guidelines for the objective evaluation of security and privacy of biometric systems have been applied to competitive unprotected systems and to the newly proposed template protection approaches for several characteristics, namely: face, iris, handshape, fingerprint, fingervein and on-line signature. In order to contribute reproducible research and allow future comparisons with other approaches, publicly available databases and systems have been used in the experimental evaluations.

7.1. Conclusions

Chapter 1 introduced the basics of biometric systems, privacy issues related to biometric systems, our perspective on the security and privacy evaluation problem, the motivation of the Thesis, and the research contributions originated from this Thesis. Chapter 2 summarized the most relevant works related to the different research lines developed in the Dissertation and which served as motivation for the work that originated the Thesis. The security evaluation and privacy methodology followed in the Thesis was presented in Chapter 3, which also described the baseline unprotected biometric systems and biometric databases used in the Thesis. In particular, a new methodology for the systematic analysis of the unlinkability of biometric templates was introduced as part of the general evaluation framework.

The experimental part of the Dissertation started in Chapter 4 with the description of two original inverse biometric methods based on optimization algorithms to reconstruct synthetic biometric samples from the information stored in the (unprotected) templates. The reconstructed

samples were subsequently used to launch attacks to academic and commercial systems. More specifically, *i*) an inverse biometrics method based on the uphill simplex algorithm was presented and used to analyse the irreversibility of three different handshape templates based on independent sets of features, and *ii*) an inverse biometric method based on genetic algorithms was proposed and used to analyse the irreversibility of iriscodes.

In order to address the security and privacy issues derived from the use and storage of unprotected templates, a new framework for template protection schemes based on Bloom Filters was presented in Chapter 5. An improved version of the original approach was first introduced, in order to increase the irreversibility of the templates, add unlinkability to the initial system, and, at the same time, preserve verification accuracy. Additionally, a methodology was developed for the estimation of the main parameters of Bloom filter based templates computation, based on a statistical analysis of the unprotected templates. Due to the higher privacy and verification accuracy granted by multi-biometric schemes, a general framework for the weighted feature level fusion of Bloom filter templates, of possibly different sizes, was proposed. The experimental evaluation showed that only at very high security operating points some verification accuracy degradation was observed, due to the inherent nature of Bloom filters. Additionally, a very high accuracy, with an EER of 0.1%, was achieved for the fusion of only two characteristics, namely face and iris. Furthermore, the unlinkability of the enhanced templates was increased for all attacking scenarios analysed with respect to the original scheme.

Finally, in Chapter 6 a new framework for template protection schemes based on Homomorphic Encryption was presented. On the one hand, regarding unimodal systems, we implemented in the encrypted domain several distance measures for fixed-length templates, namely: the Mahalanobis, Euclidean and Cosine distances. Given that some characteristics, such as on-line signature, achieve a higher verification accuracy when variable-length templates are used, a system based on a DTW implementation in the encrypted domain was also proposed. Finally, in order to achieve more secure templates and higher accuracy rates, a general multi-biometric template protection framework for feature, score and decision level fusion was described. The experimental evaluation showed that verification accuracy is preserved at all operation points, while the comparison process, being carried out in the encrypted domain, reveals no information about the underlying biometric data. Furthermore, the additional computational load due to the encryption technique was analysed, conlcuding that the comparison of fixed-length templates can be carried out on high demanding real time applications.

It should be noted that both template protection approaches offer different advantages and disadvantages. First of all, regarding verification accuracy, while the use of Bloom filter based templates can imply to some degradation for very low FMRs, Homomorphic Encryption can grant an accuracy equivalent to that of the unprotected templates at all operating points. On the other hand, whereas the implementation of complex algorithms in the encrypted domain may not be straightforward and/or lead to a high computational load within Homomorphic Encryption BTPs, Bloom filters templates can be in principle extracted form any given unprotected template, including those designed within top-ranked approaches in the state-of-the-art.

Furthermore, since the Bloom filter similarity score computation remains the same, regardless of the unprotected template considered, and is basically an efficient normalised Hamming Distance, no additional load computational is entailed. Moreover, both approaches involve different storage requirements: while Bloom filter based templates are compact (e.g., the original face templates comprising 9.4 KB are compressed to protected templates of 1.9 KB, and the original iriscode, comprising 1.25 KB, is transformed into a 4 KB protected template), the use of Homomorphic Encryption encompasses a big increase in template size: each original integer (8 to 16 bits) is encoded into 2,048 bits in the encrypted domain, yielding templates of 40 KB for the fixed-length or up to 225 MB for the variable-length on-line signature verification systems considered.

Taking into account the privacy of the subjects, Bloom filter based templates provide a permanent protection, even in the challenging scenario when an attacker is in possession of secret keys. As it has been shown, even in that case the attacker cannot invert the templates to its unprotected form (full irreversibility is provided) and a high level of unlinkability is also achieved. On the other hand, should the private or secret key of the Paillier cryptosystem be compromised, an eventual attacker could easily decrypt the protected templates to obtain its unprotected counterparts. However, such an scheme can also entail some advantages: for some applications, we may require to have access to the unprotected templates at some point, or, in the case of re-enrolment with a different key due to a database leakage, no further samples should be acquired from the subjects. Only a decryption and re-encryption would be required.

On the contrary, assuming that secret keys are not compromised, which is a reasonable assumption within cryptographic schemes, a higher level of unlinkability is provided by Homomorphic Encryption. Due to the probabilistic nature of Paillier's cryptosystem, encrypting twice a single message using the same public key will lead to different ciphertexts. As a consequence, not only the encrypted *mated* and *non-mated* score distributions obtained from comparisons of templates protected with *different* keys will overlap. The distribution of encrypted scores, obtained from *mated* and *non-mated* comparisons of templates protected with the *same* key are also expected to overlap. However, this is not the case for the Bloom filter approach: should we use the same key to protect the templates in two different systems, the score distributions would be easily separable.

In summary, the main results and contributions obtained from this Thesis are:

- The security and privacy evaluation methodology for biometric systems followed throughout the Dissertation.
- The unlinkability analysis of biometric templates proposed as part of the general evaluation protocol.
- The inverse biometrics methods developed and used for the irreversibility analysis of unprotected biometric templates: *i*) new inverse biometric attack based on the uphill simplex algorithm and *ii*) new inverse biometric method based on genetic algorithms for the reconstruction of iris images.

- The biometric template protection schemes developed and systematically evaluated in terms of the security and privacy provided: *i*) new biometric and multi-biometric template protection scheme based on Bloom filters, and *ii*) new biometric and multi-biometric template protection scheme based on Homomorphic Encryption.

- The experimental evidence of the application of the security and privacy evaluation methodology to unprotected systems based on handshape and iris.

- The experimental evidence of the application of the security and privacy evaluation methodology to protected biometric systems based on very relevant characteristics: face, iris, fingerprint, fingervein and on-line signature.

7.2. Future Work

A number of research lines arise from the work carried out in this Thesis. We consider of special interest the following ones:

- Application of the proposed security and privacy evaluation methodology to other biometric systems. In spite of the numerous biometric template protection schemes introduced in the literature [Patel *et al.*, 2015; Rathgeb and Uhl, 2011], in most cases a systematic evaluation of the accuracy degradation of the system with respect to its unprotected counterpart, or irreversibility and unlinkability analyses under realistic adversary models, are not provided. The biometric community should thus direct some efforts not only to the proposal of new biometric template protection schemes but also to the systematic and thorough evaluation of the security and privacy provided.

- Proposal of a more general unlinkability analysis framework. The described framework only takes into account one-to-one comparisons, when the attacker is in possession of two protected templates and wants to decide whether they belong to the same subject. However, other scenarios should be taken into account when analysing the unlinkability of the templates. For instance, we will further investigate the more general case when the attacker can compare a single template with a database of N different templates and decide whether any of them conceal the same identity.

- Analysis of the impact of intra-class variability on Bloom filter based schemes' accuracy. Even if verification accuracy was preserved to a great extent in the case studies analysed in the Dissertation, it could be expected that a higher intra-class variability could affect the protected systems accuracy. In fact, for the characteristic exhibiting the highest variability (i.e., face), Bloom filters should be shorter in order to be able to handle such variability and maintain verification accuracy. Therefore, the relationship between the intra-class variability and the level of protection granted will be analysed and quantified.

- Analysis of the impact of different feature extraction methods on Bloom filter based schemes' accuracy. The experimental assessment in Chapter 5 showed that Log-Gabor based schemes yielded less accuracy degradation at very low FMRs than those templates based on minutiae features. We may conclude that different behaviours can be expected when dealing with unprotected templates based on different types of features. In order to improve the accuracy rates of BTP schemes based on Bloom filters, unrelated feature extraction methods will be analysed and some guidelines as to which are the most appropriate types of features for the Bloom filter computation will be developed.

- Further analysis of the unlinkability of Homomorphic Encryption based templates. Due to the semantic security provided by such encryption scheme, it can be argued that the encrypted templates protect the security and privacy of the subject under an honest-but-curious adversary model. However, it has been shown that systems based on the Goldwasser-Micali or the Paillier cryptosystems exhibit potential weaknesses if evaluations are carried out under more challenging adversary models [Simoens *et al.*, 2012a]. Therefore, a similar evaluation should be applied to the proposed methods under the advanced model defined in Chapter 2, Sect. 2.2.1.

- Implementation of more accurate biometric verification schemes within Homomorphic Encryption BTPs. Even though Homomorphic Encryption has recently emerged as a powerful alternative to current biometric template protection schemes, and, in general, to enhance signal processing tasks where privacy is of the utmost importance [Aguilar-Melchor *et al.*, 2013; Barni *et al.*, 2015], the limitations in the number of operations which can be carried out in the encrypted domain have reduced its application to simple comparison techniques which may not be top-ranked in the state of the art. Therefore, some efforts should be directed to the implementation of more complex algorithms, yielding state-of-the-art accuracy rates.

- Development of more general multi-biometric schemes within Homomorphic Encryption BTPs. In this Dissertation we have only taken into account a simple weighted sum for the score level fusion. However, more complex fusions have shown better accuracy rates for unprotected systems [Poh and Kittler, 2012]. As a consequence, in order to make the proposed multi-biometric scheme as general as possible, further fusion rules, such as those based on quality measures [Fierrez *et al.*, 2005], will be studied.

Apéndice A

Resumen Extendido de la Tesis

Mejora de la Seguridad y la Privacidad de los Sistemas Biométricos

A.1. Resumen

La consecución de la seguridad perfecta es una utopía. Cualquier tecnología relacionada con la seguridad tiene puntos débiles que un atacante puede explotar para evadir el sistema, aunque todavía no seamos conscientes de ello. Debemos por tanto dirigir nuestros esfuerzos al desarrollo de aplicaciones cuyo nivel de seguridad haga imposible para los atacantes con recursos limitados eludir los sistemas.

Esta Tesis se centra en la mejora de la seguridad y la privacidad que ofrecen los sistemas biométricos. Dado la creciente necesidad de verificar identidades de un modo fiable y automático, la biometría ha emergido en las últimas décadas como una alternativa pujante a los métodos de autenticación tradicionales. Sin duda el reconocimiento biométrico es atractivo y útil para el público en general: olvida los PINs y contraseñas, tú eres tu propia clave. Sin embargo, la amplia implantación de sistemas de reconocimiento biométrico tanto en aplicaciones a gran escala (p.ej., el control de fronteras a nivel europeo o los sistemas de identificación nacionales) como en tareas cotidianas (p.ej., acceso a Smartphones o PCs), ha planteado serias preocupaciones acerca del uso y almacenamiento de datos tan sensibles. Tiene por tanto una gran importancia la comprensión de las amenazas que puedan afectar a dichos sistemas y analizar hasta qué punto está protegida la privacidad de los usuarios.

En este contexto, esta Tesis Doctoral pretende arrojar luz sobre el difícil problema de la evaluación de la seguridad y la privacidad de los sistemas de reconocimiento biométrico. Con este objetivo se ha llevado a cabo un análisis sistemático de la privacidad ofrecida por plantillas

no protegidas, y se han propuesto nuevos sistemas de protección de plantillas para hacer frente a los problemas de privacidad desvelados, evaluando rigurosamente la robustez frente a dichas amenazas contra la privacidad de los individuos. De este modo, el análisis experimental desarrollado en esta Disertación puede ayudar a desarrollar los actuales esfuerzos de estandarización de la evaluación de sistemas de protección de plantillas.

Esta Tesis se ha desarrollado siguiendo el *principio de seguridad a través de la transparencia de Kerckhoffs*, extensamente aplicado en otras áreas relacionadas con la seguridad como la criptografía. Este paradigma se basa en el hecho de que las vulnerabilidades existen con independencia de si han sido publicadas, y por ello aboga por hacer los sistemas de seguridad tan públicos como sea posible en lugar de mantener los algoritmos en secreto. Ello no implica que la oscuridad no ofrezca ninguna protección. Sin embargo, dicha protección es en el mejor de los casos sólo temporal. Debemos por tanto hacer todo lo posible por encontrar las amenazas y proponer soluciones que mitiguen sus efectos. Creemos que para garantizar la protección de la privacidad a la que tienen derecho los individuos, es necesario entender y evaluar las amenazas, y publicar análisis cuantitativos de su impacto en la privacidad de los sujetos con el objetivo de facilitar el desarrollo de contramedidas efectivas.

Dichos problemas de privacidad ya han sido reconocidos en la comunidad biométrica y se han propuesto numerosos sistemas de protección de plantillas para abordarlos. Sin embargo, en la mayoría de los casos no se han llevado a cabo evaluaciones rigurosas de la seguridad y la privacidad ofrecidas por esos sistemas. En esta Disertación, tras resumir los trabajos relacionados con la Tesis más relevantes, describimos la metodología de evaluación de la seguridad y la privacidad que se ha seguido durante los capítulos experimentales. Éstos están dedicados a: *i*) la evaluación de plantillas no protegidas y *ii*) la propuesta y evaluación de sistemas de protección de plantillas biométricas y multi-biométricas, centrándonos en cara, iris, huella dactilar, forma de la mano, patrones de venas y firma dinámica, usando bases de datos biométricas y bancos de pruebas públicos para hacer la investigación reproducible.

La parte experimental de la Tesis comienza con la evaluación de la seguridad y la privacidad de sistemas biométricos no protegidos. Para ello se ha analizado la irreversibilidad de las plantillas haciéndonos la siguiente pregunta: partiendo de la información almacenada en la plantilla, ¿podemos reconstruir muestras sintéticas que sean identificadas positivamente con las plantillas de referencia del sistema? Para contestar esa pregunta hemos desarrollado e implementado dos métodos de *inverse biometrics* o ingeniería inversa y hemos usado las muestras reconstruidas para lanzar ataques. Los experimentos muestran que es de hecho posible engañar sistemas basados en iris o en geometría de la mano con las muestras reconstruidas.

Para abordar los problemas de privacidad desvelados con el estudio anterior hemos propuesto un marco general para sistemas de protección de plantillas biométricas y multi-biométricas basado en Bloom filters. El sistema propuesto no sólo evita la reconstrucción de muestras sintéticas sino que también afronta un segundo grupo de preguntas relacionada con la protección de la privacidad: ¿puede alguien monitorizar mis actividades en diversos sistemas de reconocimiento biométrico? ¿Qué ocurre si la plantilla basada en, por ejemplo, mi cara, es comprometida: no

puedo volver a registrarme en un sistema con ella nunca más? Una rigurosa evaluación experimental de sistemas de verificación basada en cara, iris, huella dactilar y patrón de venas muestra que el sistema propuesto protege la privacidad de los individuos, incluso en el difícil escenario en que el atacante conoce las claves secretas del mismo. Asimismo, el sistema es robusto a ataques basados en debilidades conocidas de los algoritmos en los que se basa, preservando al mismo tiempo la precisión y la velocidad de verificación.

Finalmente, como alternativa a este sistema, presentamos un marco general para protección de plantillas biométricas y multi-biométricas basado en Encriptación Homomórfica (*Homomorphic Encryption*). La seguridad y la privacidad del sistema se han evaluado de forma análoga para huella dactilar y firma dinámica, probando que las plantillas encriptadas y todas las operaciones llevadas a cabo en el dominio encriptado no revelan ninguna información sobre la información biométrica subyacente. Además, la precisión de la verificación en el dominio encriptado es equivalente a la conseguida en el dominio no protegido, y se puede conseguir una velocidad de verificación similar usando plantillas de longitud fija.

El trabajo de investigación descrito en esta Disertación ha conducido a nuevas contribuciones que incluyen el desarrollo de: *i*) un método general para la evaluación de la seguridad y la privacidad de sistemas biométricos y, en particular, al análisis de la *unlinkability*[1] de las plantillas biométricas, *ii*) dos nuevos métodos de ingeniería inversa de plantillas biométricas no protegidas, *iii*) un nuevo sistema de protección de plantillas biométricas y multi-biométricas basado en Bloom filters, y *iv*) un nuevo sistema de protección de plantillas biométricas y multi-biométricas basado en Encriptación Homomórfica. Asimismo, se han llevado a cabo diversos estudios experimentales durante el desarrollo de la Tesis. Adicionalmente, el trabajo de investigación realizado durante la Tesis se ha complementado con la generación de diversas revisiones del estado del arte y la mejora de sistemas actuales de reconocimiento de firma.

A.2. Conclusiones

Esta Tesis Doctoral ha considerado el problema de la evaluación de la seguridad y la privacidad ofrecidas por sistemas de reconocimiento biométrico, a través de un análisis sistemático de la precisión del sistema, así como la irreversibilidad y unlinkability de las plantillas. Tras un resumen del estado del arte en inverse biometrics y protección de plantillas biométricas, se ha presentado la metodología usada durante la Tesis para la evaluación de la seguridad y la privacidad. En particular, se ha propuesto un nuevo marco para el análisis sistemático de la unlinkability de las plantillas. Asimismo, se han desarrollado nuevos métodos de inverse biometrics y protección de plantillas, para sistemas tanto biométricos como multi-biométricos. Las directrices para la evaluación objetiva de la seguridad y la privacidad de sistemas biométricos se han aplicado a sistemas no protegidos competitivos y a los nuevos sistemas propuestos de

[1] *Unlinkability* denota la imposibilidad de vincular dos plantillas, es decir, de ser capaces de decidir si ambas pertenecen al mismo individuo.

protección de plantillas para diversos rasgos, a saber: cara, iris, geometría de la mano, huella dactilar, patrones de venas y firma dinámica. Con el objetivo de hacer la investigación reproducible y permitir comparaciones con otras aproximaciones en el futuro, durante las evaluaciones experimentales se han usado bases de datos y sistemas disponibles públicamente.

El Capítulo 1 ha incluido una introducción a los sistemas biométricos, los problemas de privacidad relacionados con ellos, nuestra perspectiva sobre el problema de la evaluación de la seguridad y la privacidad, la motivación de la Tesis, y las contribuciones originadas en la misma. El Capítulo 2 ha resumido los trabajos más relevantes relacionados con las diferentes líneas de investigación desarrolladas en esta Disertación y que sirven como motivación para el trabajo que originó la Tesis. La metodología seguida en la Tesis para la evaluación de la seguridad y la privacidad se ha presentado en el Capítulo 3, en el que también se han descrito los sistemas de reconocimiento biométrico no protegidos de referencia y las bases de datos biométricas usados en esta Tesis. En particular, se ha introducido una nueva metodología para el análisis sistemático de la unlinkability de plantillas biométricas como parte del marco de evaluación general.

La parte experimental de la Disertación ha comenzado en el Capítulo 4 con la descripción de dos métodos originales de inverse biometrics, basados en algoritmos de optimización, para la reconstrucción de muestras biométricas sintéticas a partir de la información almacenada en las plantillas (no protegidas). Las muestras reconstruidas se han usado a continuación para lanzar ataques contra sistemas académicos y comerciales. En particular, *i*) se ha presentado un método de inverse biometrics basado en el algoritmo conocido como uphill simplex y un generador de imágenes de manos, y se ha usado para analizar la irreversibilidad de tres plantillas diferentes basadas en conjuntos de características distintas, y *ii*) se ha propuesto un método de inverse biometrics basado en un algoritmo genético y se ha usado para analizar la irreversibilidad de los iriscodes.

Con el objetivo de abordar los problemas de seguridad y privacidad derivados del uso y almacenamiento de plantillas no protegidas, se ha presentado en el Capítulo 5 un nuevo marco para sistemas de protección de plantillas basados en Bloom filters. En primer lugar se ha introducido una versión mejorada con respecto a la aproximación original, en la que se ha aumentado la irreversibilidad de las plantillas, se ha añadido unlinkability al sistema original, y, al mismo tiempo, se ha mantenido la precisión de verificación. Adicionalmente, se ha desarrollado una metodología para la estimación de los principales parámetros en la extracción de plantillas basadas en Bloom filters, basada a su vez en un análisis estadístico de las plantillas no protegidas. Dada la mayor privacidad y precisión en la verificación ofrecida por los sistemas multi-biométricos, se ha propuesto un marco general para una fusión ponderada a nivel de característica de plantillas basadas en Bloom filters, posiblemente de diferentes tamaños. La evaluación experimental ha mostrado que sólo en puntos de trabajo de muy alta seguridad se aprecia alguna degradación de la precisión del sistema, debido a la naturaleza inherente de los Bloom filters. Se ha conseguido asimismo una gran precisión, con un EER del 0.1%, con la fusión de sólo dos rasgos, a saber, cara e iris. Adicionalmente, se ha incrementado la unlinkability de las plantillas mejoradas con respecto a la aproximación original para todos los escenarios de ataque analizados.

Finalmente, en el Capítulo 6 se ha presentado un nuevo marco para los sistemas de protección de la plantillas basado en Encriptación Homomórfica. Por un lado, hemos implementado en el dominio encriptado diversas funciones de distancia para plantillas de longitud fija, a saber: las distancias de Mahalanobis, Euclídea y Coseno. Dado que para algunos rasgos, como la firma dinámica, se obtiene una mayor precisión usando plantillas de longitud variable, se ha propuesto también un sistema basado en la implementación de DTW en el dominio encriptado. Finalmente, para conseguir plantillas más seguras y una mayor precisión en la verificación, se ha descrito un marco general para la protección de plantillas multi-biométricas para fusiones a nivel de característica, puntuación y decisión. La evaluación experimental ha mostrado que la precisión de la verificación se mantiene para todos los puntos de trabajo, mientras que el proceso de comparación, al ser llevado a cabo en el dominio encriptado, no revela ninguna información sobre los datos biométricos subyacentes. Se ha analizado asimismo la carga computacional añadida por el proceso de encriptación, concluyendo que la comparación de plantillas de longitud fija se puede realizar en aplicaciones en tiempo real.

Cabe destacar que ambos sistemas de protección de plantillas ofrecen distintas ventajas y desventajas. En primer lugar, en cuanto a la precisión de los sistemas, mientras que el uso de Bloom filters puede implicar cierta degradación para FMRs muy bajas, la Encriptación Homomórfica puede garantizar una precisión equivalente a la obtenida con las plantillas no protegidas para todos los puntos de trabajo. Por otro lado, mientras que la implementación de algoritmos complejos en el dominio encriptado pues no ser directa y/o conducir a una mayor carga computacional en BTPs basados en Encriptación Homomórfica, las plantillas basadas en Bloom filters pueden en principio extraerse de cualquier plantilla no protegida, incluidas aquéllas diseñadas para los esquemas a la cabeza del estado del arte. Asimismo, dado que el cálculo de las puntuaciones de similitud entre Bloom filters se reduce a una Distancia de Hamming ponderada, muy eficiente, independientemente de la plantilla no protegida utilizada, no se añade ninguna carga computacional. Además, ambos enfoques tienen distintos requisitos de almacenamiento: mientras que las plantillas basadas en Bloom filters son compactas (p.ej., las plantillas de cara originales, que comprenden 9.4 KB, con comprimidas a plantillas de 1.9 KB, y el iriscode original, que comprende 1.25 KB, se transforma en una plantilla protegida de 4 KB), el uso de Encriptación Homomórfica acarrea un considerable aumento del tamaño de las plantillas: cada entero (8 a 16 bits) se codifica con 2,048 bits en el dominio encriptado, dando lugar a plantillas de 40 KB para el caso de longitud fija, y de hasta 225 MB para las de longitud variable, en los sistemas de verificación de firma dinámica considerados.

Teniendo en cuenta la privacidad de los individuos, las plantillas basadas en Bloom filters ofrecen una protección permanente, incluso en el desafiante escenario en el que el atacante conoce las claves secretas. Como se ha probado, incluso en ese caso el atacante no puede invertir la plantilla a su forma no protegida (se ofrece una irreversibilidad completa) y se consigue también un alto nivel de unlinkability. Por otro lado, si la clave privada del criptosistema de Paillier es comprometida, un atacante podría fácilmente desencriptar las plantillas para obtener sus homólogas sin proteger. Este esquema sin embargo puede también conllevar ciertas ventajas:

para algunas aplicaciones, puede requerirse el acceso a las plantillas sin proteger en algún momento, o, en caso de re-registro con otra clave tras una filtración en la base de datos, no se tendrían que adquirir nuevas muestras de los sujetos. Bastaría con desencriptar y re-encriptar las plantillas.

Al contrario, asumiendo que las claves secretas no han sido comprometidas, una suposición razonable en sistemas criptográficos, la Encriptación Homomórfica ofrece un mayor nivel de unlinkability. Dada la naturaleza probabilística del criptosistema de Paillier, si se encripta dos veces un mismo mensaje usando la misma clave pública, el resultado son dos mensajes encriptados distintos. Como consecuencia, no sólo observamos un solapamiento entre las distribuciones de puntuaciones encriptadas obtenidas de comparaciones *mated* y *non-mated* entre plantillas protegidas con *distintas* claves. Las distribuciones de puntuaciones encriptadas, obtenidas de comparaciones *mated* y *non-mated* entre plantillas protegidas con la *misma* clave también cabría esperar que se solaparan. Sin embargo, esto no se extiende a los Bloom filters: si usamos la misma clave para proteger plantillas en dos sistemas diferentes, las distribuciones de puntuaciones serán fácilmente separables.

En resumen, los principales resultados y contribuciones obtenidos en esta Tesis son:

- La metodología de evaluación de la seguridad y la privacidad de los sistemas de reconocimiento biométrico seguida durante la Disertación.
- El análisis de la unlinkability de las plantillas biométricas propuesto como parte del protocolo general de evaluación.
- Los métodos de inverse bimetrics desarrollados y usados en el análisis de la irreversibilidad de las plantillas biométricas no protegidas: *i*) nuevo ataque de inverse biometrics basado en el uphill simplex y *ii*) nuevo método de inverse biometrics basado en algoritmos genéticos para la reconstrucción de iris.
- Sistemas de protección de plantillas biométricas desarrollados y evaluados sistemáticamente en cuanto a la seguridad y privacidad ofrecidas: *i*) nuevo esquema de protección de plantillas biométricas y multi-biométricas basado en Bloom filters y *ii*) nuevo esquema de protección de plantillas biométricas y multi-biométricas basado en Encriptación Homomórfica.
- Las evidencias experimentales de la aplicación de la metodología de evaluación de la seguridad y la privacidad a sistemas no protegidos basados en mano e iris.
- Las evidencias experimentales de la aplicación de la metodología de evaluación de la seguridad y la privacidad a sistemas de protección de plantillas basado en rasgos muy relevantes: cara, iris, huella dactilar, patrones de venas y firma dinámica.

A.3. Líneas de Trabajo Futuro

Se proponen las siguientes líneas de trabajo futuro relacionadas con el trabajo desarrollado en esta Tesis Doctoral:

- Aplicación de la metodología de evaluación de la seguridad y la privacidad propuesta a otros sistemas de reconocimiento biométrico. A pesar de los numerosos esquemas de protección de plantillas presentes en la literatura [Patel *et al.*, 2015; Rathgeb and Uhl, 2011], en la mayoría de los casos no se incluyen evaluaciones sistemáticas de la degradación de la precisión en la verificación con respecto a los sistemas sin proteger, o los análisis de irreversibilidad y unlinkability se llevan a cabo bajo modelos de amenazas no realistas. La comunidad biométrica debe por tanto dirigir sus esfuerzos no sólo a proponer nuevos sistemas de protección de plantillas sino también a la evaluación sistemática y rigurosa de la seguridad y la privacidad ofrecidas.

- Propuesta de un marco de análisis de la unlinkability más general. El marco descrito sólo tiene en cuenta comparaciones uno-a-uno, cuando el atacante obtiene dos plantillas protegidas y quiere decidir sin pertenecen a la misma persona. Sin embargo, se deberían tener en cuenta otros escenarios a la hora de analizar la unlinkability de las plantillas. Por ejemplo, investigaremos en mayor profundidad el caso más general en el que el atacante puede comparar una única plantilla con una base de datos de N plantillas y decidir si alguna de ellas esconde la misma identidad.

- Análisis del impacto de la variabilidad intra-clase en la precisión de los sistemas basados en Bloom filters. Aunque la precisión en la verificación se mantiene en un alto grado en los casos de estudio analizados en esta Disertación, cabría esperar que una mayor variabilidad intra-clase pudiera afectar la precisión del sistema protegido. De hecho, para el rasgo con una mayor variabilidad (la cara), los Bloom filters deben ser más cortos para poder hacer frente a dicha variabilidad y mantener la precisión. Por lo tanto, se analizará y cuantificará la relación entre la variabilidad intra-clase y el nivel de protección garantizado.

- Análisis del impacto de diferentes métodos de extracción de características en la precisión de los sistemas basados en Bloom filters. La evaluación experimental del Capítulo 5 muestra que los esquemas basados en filtros LogGabor consiguen una menor degradación de la precisión para Tasas de Falsa Aceptación (FMR) muy bajas que aquéllos basados en minucias. Podríamos por tanto concluir que cabe esperar diferentes comportamientos cuando trabajamos con plantillas basadas en distintos tipos de características. Con el fin de mejorar la tasas de error de los esquemas basados en Bloom filters, analizaremos diversos métodos de extracción de características y se desarrollarán pautas sobre los tipos de características más apropiados para el cálculo de los Bloom filters.

- Análisis más detallado de la unlinkability de las plantillas basadas en Encriptación Homomórfica. Debido a la seguridad semántica ofrecida por los sistemas de encriptación,

puede argumentarse que las plantillas encriptadas protegen la seguridad y la privacidad del individuo bajo un modelo honesto pero curioso (*honest-but-curious adversary model*). Sin embargo, se ha probado que sistemas basados en los criptosistemas de Goldwasser-Micali o Paillier muestran debilidades si las evaluaciones se llevan a cabo bajo modelos más severos [Simoens *et al.*, 2012a]. Debemos por tanto realizar una evaluación similar de los métodos propuestos bajo el model avanzado definido en el Capítulo 2, Sec. 2.2.1.

- Implementación de sistemas de reconocimiento biométrico más precisos en el marco de la Encriptación Homomórfica. A pesar de que la Encriptación Homomórfica ha surgido recientemente como una potente alternativa a los esquemas actuales de protección de plantillas, y, en general, para mejorar tareas relacionado con el procesado de señal en las que la privacidad tiene una gran importancia [Aguilar-Melchor *et al.*, 2013; Barni *et al.*, 2015], las limitaciones en el número de operaciones que pueden llevarse a cabo en el dominio encriptado han reducido su aplicación a técnicas de comparación simples que pueden no estar a la cabeza del estado del arte. Es por ello que debemos dirigir nuestros esfuerzos a la implementación de algoritmos más complejos, que consigan tasas de error en el estado del arte.

- Desarrollo de esquemas más generales de protección de plantillas multi-biométricas en el marco de la Encriptación Homomórfica. En esta Disertación sólo hemos tenido en cuenta una suma ponderada para la fusión a nivel de puntuación. Sin embargo, otras fusiones más complejas han obtenido mayor precisión en sistemas no protegidos [Poh and Kittler, 2012]. De este modo, con el objetivo de hacer el marco de protección de plantillas multi-biométricas lo más general posible, estudiaremos otras reglas de fusión, como aquéllas basadas en medidas de calidad [Fierrez *et al.*, 2005].

References

Signal processing in the encrypted domain, ieee signal processing magazine, 2013. 32

Biometrics security and privacy protection, ieee signal processing magazine, 2015. 7

N. Abe, S. Yamada, and T. Shinzaki. Irreversible fingerprint template using minutiae relation code with bloom filter. In *Proc. Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS)*, 2015. 28

A. Adler. Sample images can be independently restored from face recognition templates. In *Proc. Canadian Conf. on Electrical and Computer Engineering (CCECE)*, volume 2, pages 1163–1166, 2003. 21, 22, 23

A. Adler. Images can be regenerated from quantized biometric match score data. In *Proc. Canadian Conf. on Electrical and Computer Engineering (CCECE)*, pages 469–472, 2004. 22, 23

A. Adler. Vulnerabilities in biometric encryption systems. In *Proc. IAPR Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 1100–1109. Springer LNCS-3546, 2005. 2

C. Aguilar-Melchor, S. Fau, C. Fontaine, G. Gogniat, and R. Sirdey. Recent advances in homomorphic encryption: A possible future for signal processing in the encrypted domain. *IEEE Signal Processing Magazine*, 30(2):108–117, 2013. 32, 155, 164

F. Alonso-Fernandez and J. Bigun, editors. *Proc. of the 8th International Conference on Biometrics (ICB)*, 2016. 7

R. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2001. 140, 141

A. Anjos, L. E. Shafey, *et al.* Bob: a free signal processing and machine learning toolbox for researchers. In *Proc. ACM Int. Conf. on Multimedia (MM)*, pages 1449–1452, 2012. 52

ANSI-NIST. ANSI x9.84-2001, biometric information management and security, 2001. 43, 111

ANSI/NIST. NIST ITL american national standards for biometrics, 2009. http://fingerprint.nist.gov/standard/. 2, 76, 86

E. Argones-Rua, E. Maiorana, J. L. Alba-Castro, and P. Campisi. Biometric template protection using universal background models: An application to online signature. *IEEE Trans. on Information Forensics and Security*, 7(1):269–282, 2012. 30, 43

B. S. Atal. Automatic recognition of speakers from their voices. *Proc. of IEEE*, 64:460–475, 1976. 1, 39

J. E. Baker. Reducing bias and inefficiency in the selection algorithm. In *Proc. Int. Conf. on Genetic Algorithms and their Application (ICGAA)*, pages 14 – 21. L. Erlbaum Associates Inc., 1987. 68

M. Barni, T. Bianchi, D. Catalano, M. di Raimondo, R. D. Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, A. Piva, and F. Scotti. A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates. In *Proc. Int. Conf. on Biometrics: Theory Applications and Systems (BTAS)*, pages 1–7, 2010. 3, 32, 33

M. Barni, G. Droandi, and R. Lazzeretti. Privacy protection in biometric-based recognition systems: A marriage between cryptography and signal processing. *IEEE Signal Processing Magazine*, 32(5):66–76, 2015. 6, 7, 32, 119, 121, 155, 164

BBfor2, 2010. BBfor2: Bayesian Biometrics for Forensics, FP7-ITN-2008-238803. (http://www.bbfor2.net/). 1

BC. Biometrics consortium, 2009. (http://www.biometrics.org/). 1

C. Bergman. *Advances in biometrics*, chapter Match-on-card for secure and scalable biometric authentication, pages 407–421. Springer, 2008a. 3

C. Bergman. *Advances in Biometrics: sensors, algorithms and systems*, chapter Match-on-card for secure and scalable biometric authentication, pages 407–422. Springer, 2008b. 89

R. Beveridge, J. Phillips, D. Bolme, B. Draper, G. Givens, Y. M. Lui, M. N. Teli, H. Zhang, W. T. Scruggs, K. Bowyer, P. Flynn, and S. Cheng. The challenge of face recognition from digital point-and-shoot cameras (pasc). In *Porc. Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS)*, 2013. 1

BF. The biometric foundation, 2009. (http://www.biometricfoundation.org/). 1

BI. Biometrics institute, 2009. (http://www.biometricsinstitute.org/). 1

T. Bianchi, S. Turchi, A. Piva, R. Labati, V. Piuri, and F. Scotti. Implementing fingercode-based identity matching in the encrypted domain. In *Proc. Int. Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS)*, pages 15–21, Sept 2010. 32

J. Bigun. *Vision with Direction: A Systematic Introduction to Image Processing and Computer Vision*. Springer, 2006. 14

BioAPI. The BioAPI consortium, 2009. http://www.bioapi.org. 2

BioAPI Consortium. BioAPI specification (version 1.1), March 2001. www.bioapi.org/Downloads/BioAPI123

BioSec, 2004. Biometrics and Security, FP6 IP IST-2002-001766. (http://www.biosec.org/). 1

Biosecure, 2007. Biometrics for Secure Authentication, FP6 NoE IST-2002-507634. (http://www.biosecure.info/). 1

M. Blanton and P. Gasti. Secure and efficient protocols for iris and fingerprint identification. In *Proc. European Symposium on Research in Computer Security (ESORICS)*, pages 190–209, 2011. 32, 33

B. Bloom. Space/time tradeoffs in hash coding with allowable errors. *Communications of the ACM*, 13(7):422–426, 1970. 27

T. Boult. Robust distance measures for face-recognition supporting revocable biometric tokens. In *Proc. Int. Conf. on Automatic Face and Gesture Recognition (FGR)*, pages 560–566, 2006. ISBN 0-7695-2503-2. 27

T. E. Boult, W. J. Scheirer, and R. Woodworth. Revocable fingerprint biotokens: Accuracy and security analysis. In *Proc. Int. Conf. on Computer Vision and Pattern Recognition (CVPR)*, pages 1–8, 2007. 27

K. Bowyer, A. Ross, R. Beveridge, P. Flynn, and M. Pantic, editors. *Proc. of 7th International Conference Biometrics: Theory, advances and systems (BTAS)*, 2015. IEEE. 1, 7

J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zemor. Optimal iris fuzzy sketches. In *Proc. Int. Conf. on Biometrics: Theory, Applications, and Systems (BTAS)*, pages 1–6, 2007. 29, 30

J. Bringer, H. Chabanne, M. Favre, A. Patey, T. Schneider, and M. Zohner. GSHADE: Faster privacy-preserving distance computation and biometric identification. In *Proc. ACM Workshop on Information Hiding and Multimedia Security*, pages 187–198, 2014a. 33

J. Bringer, H. Chabanne, and A. Patey. Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends. *IEEE Signal Processing Magazine*, 30(1):42–52, 2013. 32

J. Bringer, M. Favre, C. Pelle, and H. de Saxce. Fuzzy vault and template-level fusion applied to a binary fingerprint representation. In *Proc. Int. Conf. of the Biometrics Special Interest Group (BIOSIG)*, pages 1–4, 2014b. 35, 36

J. Bringer, C. Morel, and C. Rathgeb. Security analysis of bloom filter-based iris biometric template protection. In *Proc. Int. Conf. on Biometrics (ICB)*, pages 527–534, 2015. 28, 94, 103, 104, 112, 118

A. Broder and M. Mitzenmacher. Network applications of bloom filters: A survey. *Internet Mathematics*, 1(4): 485–509, 2005. 27

J. Burgues, J. Fierrez, D. Ramos, and J. Ortega-Garcia. Feature selection in a hand geometry recognition system. In *Proc. of BioID-Multicomm*, pages 325–332, 2009. 50, 73

J. Bustard. The impact of eu privacy legislation on biometric system deployment: Protecting citizens but constraining applications. *IEEE Signal Processing Magazine*, 32(5):101–108, 2015. 6

BWG. Biometric security concerns, v1.0. Technical report, CESG, UK Government, 2003. 10

BWG. Communications-electronics security group (CESG) – biometric working group (BWG) (UK government), 2009. http://www.cesg.gov.uk/policy_technologies/biometrics/index.shtml. 2, 10

P. Campisi, editor. *Security and Privacy in Biometrics*. Springer, 2013. 24

A. M. P. Canuto, F. Pintro, and J. C. Xavier-Junior. Investigation fusion approaches in multi-biometric cancellable recognition. *Expert Systems with Applications*, 40:1971–1980, 2013. 35, 36

R. Cappelli. *Handbook of Fingerprint Recognition*, chapter Synthetic Fingerprint Generation, pages 203–231. Springer, 2003. 19, 21

R. Cappelli, D. Maio, A. Lumini, and D. Maltoni. Fingerprint image reconstruction from standard templates. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 29:1489–1503, September 2007. 21, 22, 70

R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain. Performance evaluation of fingerprint verification systems. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 28(1):3–18, 2006. 1

D. Catalano, R. Gennaro, and N. Howgrave-Graham. The bit security of paillier's encryption scheme and its applications. In *Proc. EUROCRYPT*, pages 229–243, 2001. 142

A. Cavoukian and A. Stoianov. Biometric encryption: The new breed of untraceable biometrics. In *Biometrics: fundamentals, theory, and systems*. Wiley, 2009. 43

R. Chellappa, J. Kittler, A. Kumar, B. Lovell, S. Sarkar, N. Nemon, and Z. Sun, editors. *Proc. First International Conference on Identity, Security and Behavior Analysis (ISBA)*, 2015. 1

S. Cimato, M. Gamassi, V. Piuri, R. Sassi, and F. Scotti. Privacy-aware biometrics: Design and implementation of a multimodal verification system. In *Proc. IEEE Ann. Conf. Computer Security Applications*, 2008. 36

T. C. Clancy, N. Kiyavash, and D. J. Lin. Secure smartcardbased fingerprint authentication. In *Proc. of ACM SIGMM workshop on Biometrics methods and applications*, pages 45–52, 2003. 31

T. F. Cootes, G. J. Edwards, and C. J. Taylor. Active appearance models. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 23:681–685, 2001. 61, 73

T. F. Cootes, C. J. Taylor, D. H. Cooper, and J. Graham. Active shape models - their training and application. *Computer Vision and Image Undersanding*, 61(1):38–59, 1995. 61, 73

COST. COST 2101: Biometrics for identity documents and smart cards, 2007. http://cost2101.org/. 1

J. Cui, Y. Wang, J. Huang, T. Tan, and Z. Sun. An iris image synthesis method based on pca and super-resolution. In *Proc. Int. Conf. on Pattern Recognition (ICPR)*, pages 471–474, 2004. 19, 21

J. Daugman. How iris recognition works. *Circuits and Systems for Video Technology, IEEE Transactions on*, 14 (1):21–30, 2004. 51, 98

B. D. Decker, S. Katzenbeisser, and J.-H. Hoepman, editors. *Proc. of the 31st International Information Security and Privacy Conference (IFIP SEC)*, 2016. 7

DoD. Biometrics Management Office, Department of Defense, USA, 2009. http://www.biometrics.dod.mil/. 2

R. O. Duda, P. E. Hart, and D. G. Stork. *Pattern Classification.* Wiley, 2001. 14, 92, 120

N. Duta. A survey of biometric technology based on hand shape. *Pattern Recognition*, 42:2797–2806, 2009. 50

T. Dutoit. *An introduction to text-to-speech synthesis.* Kluwer Academic Publishers, 2001. 19

EAB, 2012. European Association for Biometrics. (http://eab.org/). 1

EAB-CITeR. European Cooperative Identification Technology Research Consortium, 2015. 1

Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft. Privacy-preserving face recognition. In *Proc. Int. Symposium on Privacy Enhancing Technologies (PETS)*, pages 235–253. Springer, 2009. 32, 33

European Association for Biometrics (EAB). 4th Seminar on Biometrics in Banking and Payments. 2015. 2

European Comission. Smart borders, 2013. URL `http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/index_en.htm`. 2

European Parliament. Directive IP/12/46 of the European Parliament and of the Council of January 2012 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 2012. URL `http://europa.eu/rapid/press-release_IP-15-6321_en.htm`. 6

European Parliament. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Oct. 1995. 6

C. Fang, Q. Li, and E. C. Chang. Secure sketch for multiple secrets. In *Proc. Int. Conf. on Applied Cryptography and Network Security*, pages 367–383, 2010. 36

H. Feng and C. C. Wah. Private key generation from on-line handwritten signatures. *Information Management & Computer Security*, 10(4):159–164, 2002. 30, 31

N. Ferguson and B. Schneier. *Practical Cryptography*. Wiley New York, 2003. 14, 120

M. Ferrara, D. Maltoni, and R. Cappelli. A two-factor protection scheme for mcc fingerprint templates. In *Proc. Int. Conf. of the Biometrics Special Interest Group (BIOSIG)*, pages 1–8, 2014. 7, 43, 44

M. A. Ferrer and A. Morales. Hand-shape biometrics combining the visible and short-wave infrared bands. *IEEE Trans. on Information Forensics and Security*, 6(4):1305–1314, 2011. 50, 61, 71, 73

M. A. Ferrer, A. Morales, C. M. Travieso, and J. B. Alonso. Low cost multimodal biometric identification system based on hand geometry, palm and finger print texture. In *Proc. IEEE Int. Carnahan Conf. on Security Technology (ICCST)*, 2007. 54, 71

J. Fierrez, J. Galbally, J. Ortega-Garcia, M. R. Freire, F. Alonso-Fernandez, D. Ramos, D. T. Toledano, J. Gonzalez-Rodriguez, J. A. Siguenza, J. Garrido-Salas, E. Anguiano, G. G. de Rivera, R. Ribalda, M. Faundez-Zanuy, J. A. Ortega, V. Cardeñoso-Payo, A. Viloria, C. E. Vivaracho, Q. I. Moro, J. J. Igarza, J. Sanchez, I. Hernaez, C. Orrite-Uruñuela, F. Martinez-Contreras, and J. J. Gracia-Roche. BiosecurID: a multimodal biometric database. *Pattern Analysis and Applications*, 13:235–246, 2009. 56, 136

J. Fierrez, D. Garcia-Romero, and J. Ortega-Garcia, J.and Gonzalez-Rodriguez. Adapted user-dependent multimodal biometric authentication exploiting general information. *Pattern Recognition Letters*, 26(16):2628–2639, 2005. 155, 164

J. Fierrez, A. Kumar, M. Vatsa, R. Veldhuis, and J. Ortega-Garcia, editors. *Proc. of 6th International Conference on Biometrics (ICB)*, 2013. IEEE. 1

J. Fierrez and J. Ortega-Garcia. *On-line signature verification*, chapter Handbook of biometrics, pages 189–209. Springer, 2008. 20

S. Fomel and J. F. Claerbout. Reproducible research. *Computing in Science & Engineering*, 11(1):5–7, 2009. 11

C. Fontaine and F. Galand. A survey of homomorphic encryption for nonspecialists. *EURASIP Journal on Information Security*, 2007:1–15, 2007. 14, 32, 120

M. R. Freire, J. Fierrez, J. Galbally, and J. Ortega-Garcia. Biometric hashing based on genetic selection and its application to on-line signatures. In *Proc. Int. Conf. on Biometrics (ICB)*, pages 1134–1143, 2007. 31

M. R. Freire, J. Fierrez, and J. Ortega-Garcia. Dynamic signature verification with template protection using helper data. In *Proc. Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1713–1716, 2008. 31

J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia, and D. Maio. An evaluation of direct and indirect attacks using fake fingers generated from ISO templates. *Pattern Recognition Letters*, 31:725–732, 2010a. 22

J. Galbally, M. Diaz-Cabrera, M. A. Ferrer, M. Gomez-Barrero, A. Morales, and J. Fierrez. On-line signature recognition through the combination of real dynamic data and synthetically generated static data. *Pattern Recognition*, 48:2921–2934, 2015. 20

J. Galbally, J. Fierrez, M. Martinez-Diaz, and J. Ortega-Garcia. Improving the enrollment in dynamic signature verification with synthetic samples. In *Proc. IAPR Int. Conf. on Document Analysis and Recognition (ICDAR)*, 2009. 20

J. Galbally, J. Fierrez, J. Ortega-Garcia, and R. Plamondon. Synthetic on-line signature generation. Part II: Experimental validation. *Pattern Recognition*, 45:2622–2632, 2012a. 19, 21

J. Galbally, C. McCool, J. Fierrez, and S. Marcel. On the vulnerability of face verification systems to hill-climbing attacks. *Pattern Recognition*, 43:1027–1038, 2010b. 22, 23, 122

J. Galbally, R. Plamondon, J. Fierrez, and J. Ortega-Garcia. Synthetic on-line signature generation. Part I: Methodology and algorithms. *Pattern Recognition*, 45:2610–2621, 2012b. 19

J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia. Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms. *Computer Vision and Image Understanding*, 117(10):1512–1525, 2013. DOI http://dx.doi.org/10.1016/j.cviu.2013.06.003. 19, 39, 59

A. Goh and D. C. L. Ngo. Computation of cryptographic keys from face biometrics. In *Proc. Communications and Multimedia Security*, pages 1–13, 2003. 28

D. Goldberg. *The design of innovation: lessons from and for competent genetic algorithms.* Kluwer Academic Publishers, 2002. 84

D. E. Goldberg. *Genetic Algorithms in Search Optimization and Machine Learning.* Addison Wesley, 1989. 66, 84

S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of computer and system sciences*, 28(2):270–299, 1984. 14, 120, 123

M. Gomez-Barrero, J. Galbally, and J. Fierrez. Efficient software attack to multimodal biometric systems and its application to face and iris fusion. *Pattern Recognition Letters*, 36:243–253, 2014a. 122, 141, 149

M. Gomez-Barrero, J. Galbally, and J. Fierrez. Variable-length template protection based on homomorphic encryption with application to signature biometrics. In *Proc. Int. Workshop on Biometrics and Forensics (IWBF)*, 2016a. 120

M. Gomez-Barrero, J. Galbally, J. Fierrez, and J. Ortega-Garcia. Hill-climbing attack based on the uphill simplex algorithm and its application to signature verification. In *Proc. European Workshop on Biometrics and Identity Management (BioID)*, pages 83–94. LNCS-6583, 2011. 61, 63, 73

M. Gomez-Barrero, J. Galbally, E. Maiorana, P. Campisi, and J. Fierrez. Fixed-length template protection based on homomorphic encryption with application to signature biometrics. In *Proc. Conf. on Computer Vision and Pattern Recognition (CVPR)*, 2016b. Submitted. 120

M. Gomez-Barrero, J. Galbally, A. Morales, *et al.* A novel hand reconstruction approach and its application to vulnerability assessment. *Information Sciences*, 268:103–121, 2014b. 19, 39, 59

M. Gomez-Barrero, J. Galbally, A. Morales, M. A. Ferrer, J. Fierrez, and J. Ortega-Garcia. Inverse biometrics: A case study in hand geometry authentication. In *Proc. Int. Conf. on Pattern Recognition (ICPR)*, pages 1281–1284, 2012a. 59

M. Gomez-Barrero, J. Galbally, P. Tome-Gonzalez, and J. Fierrez. On the vulnerability of iris-based systems to software attacks based on genetic algorithms. In *Proc. Iberoamerican Conf. on Pattern Recognition (CIARP)*, pages 114–121, 2012b. 86

M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fie. Multi-biometric template protection based on homomorphic encryption. *IEEE Trans. on Information Forensics and Security*, 2016c. Submitted. 19, 120

M. Gomez-Barrero, C. Rahtgeb, J. Galbally, C. Busch, and J. Fierrez. Unlinkable and irreversible biometric template protection based on bloom filters. *Information Sciences*, 2016d. 39, 92

M. Gomez-Barrero, C. Rathgeb, , G. L. R. Ramachandra, J. Galbally, and C. Busch. General framework for multi-biometric template protection based on bloom filters. *Information Fusion*, 2016e. 19, 92

M. Gomez-Barrero, C. Rathgeb, J. Galbally, J. Fierrez, and C. Busch. Protected facial biometric templates based on local gabor patterns and adaptive bloom filters. In *Proc. Int. Conf. on Pattern Recognition (ICPR)*, pages 4483–4488, 2014c. 92, 106, 109

R. C. Gonzalez and R. E. Woods. *Digital Image Processing*. Prentice Hall, 2006. 14, 92, 120

J. Gonzalez-Rodriguez, A. Drygajlo, D. Ramos-Castro, M. Garcia-Gomar, and J. Ortega-Garcia. Robust estimation, interpretation and assessment of likelihood ratios in forensic speaker recognition. *Computer Speech & Language*, 20(2):331–355, 2006. ISSN 0885-2308. 47

Government of India. Unique identification authority of india, 2012. URL `https://uidai.gov.in/`. 2

Government of Spain. URL `http://www.dnielectronico.es/`. 89

P. Grother, E. Tabassi, G. W. Quinn, and W. Salamon. IREX I: Performance of iris recognition algorithms on standard images. Technical report, National Institute of Standards and Technology, 2009. 51

M. Günther, R. Wallace, and S. Marcel. An open source framework for standardized comparisons of face recognition algorithms. In *Proc. European Conf. on Computer Vision (ECCV)*, volume 7585 of *LNCS*, pages 547–556, 2012. 52

F. Hao, R. Anderson, and J. Daugman. Combining crypto with biometrics effectively. *IEEE Trans. on Computers*, 55(9):1081–1088, 2006. ISSN 0018-9340. 29, 30

J. Hermans, B. Mennink, and R. Peeters. When a bloom filter is a doom filter: Security assessment of a novel iris biometric. In *Proc. Int. Conf. of the Biometrics Special Interest Group (BIOSIG)*, 2014. 28, 94, 104, 118

C. J. Hill. Risk of masquerade arising from the storage of biometrics. Master's thesis, Australian National University, 2001. 2, 21, 22

B. Huang, Y. Dai, R. Li, D. Tang, and W. Li. Finger-vein authentication based on wide line detector and pattern normalization. In *Proc. Int. Conf. on Pattern Recognition (ICPR)*, pages 1269–1272, 2010. 52

IBIA. International biometric industry association, 2009. (http://www.ibia.org/association/). 2

ICAO. ICAO document 9303, part 1, volume 2: Machine readable passports - specifications for electronically enabled passports with biometric identification capability, 2006. 89

T. Ignatenko and F. Willems. Achieving secure fuzzy commitment scheme for optical pufs. In *Proc. Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, pages 1185–1188, 2009a. 29

T. Ignatenko and F. Willems. Biometric systems: Privacy and secrecy aspects. *IEEE Trans. on Information Forensics and Security*, 4(4):956 – 973, 2009b. 31

T. Ignatenko and F. Willems. Information leakage in fuzzy commitment schemes. *IEEE Trans. on Information Forensics and Security*, 2(5):337–348, 2010. 31

ILO, 2006. ILO SID-0002, "Finger Minutiae-Based Biometric Profile for Seafarers' Identity Documents," Int'l Labour Organization. 89

International Biometric Group. Generating images from templates. White paper, 2002. 21

International Biometric Group. Biometrics market and industry report 2009-2014. Technical report, 2009. http://www.biometricgroup.com. 2

ISO/IEC JTC 1/SC 27. IT security techniques, 2009. http://www.jtc1.org/sc27/. 2

ISO/IEC JTC 1/SC 37. Biometrics, 2009. http://www.jtc1.org/sc37/. 2

ISO/IEC JTC1 SC 37 Biometrics. *ISO/IEC 19794-2:2011, Information technology – Biometric data interchange formats – Part 2: Finger minutiae data*. International Organization for Standardization, 2011. 22

ISO/IEC JTC1 SC27 IT Security Techniques. ISO/IEC 19792:2009, information technology - security techniques - security evaluation of biometrics., 2009. 3

ISO/IEC JTC1 SC27 IT Security Techniques. *ISO/IEC 24745:2011. Information Technology - Security Techniques - Biometric Information Protection*. International Organization for Standardization, 2011. 3, 7, 8, 11, 41, 57, 91, 105, 117, 118, 119, 148, 149

ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC 19795-1:2006. Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework*. International Organization for Standardization, 2006. 41

ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC TR 24722:2007. Information Technology – Multimodal and other multibiometric fusion*. International Organization for Standardization, 2007. 33, 117, 148

ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC WD 30136, Performance Testing of Biometric Template Protection Schemes*. International Organization for Standardization, 2015. 3, 10

A. Jain, A. Ross, and K. Nandakumar. *Introduction to Biometrics*. Springer, 2011. 1, 2, 4, 5, 14, 40

A. K. Jain, R. P. W. Duin, and J. Mao. Statistical pattern recognition: a review. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 22(1):4–37, 2000. 40

A. K. Jain, K. Nandakumar, and A. Ross. Score normalization in multimodal biometric systems. *Pattern Recognition*, 38:2270–2285, 2005. 54, 132

A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti. FingerCode: a filterbank for fingerprint representation and matching. In *Proc. Conf. on Computer Vision and Pattern Recognition (CVPR)*, 1999. 32, 53

A. K. Jain, A. Ross, and P. Flynn, editors. *Handbook of biometrics*. Springer, 2008. 1

A. K. Jain, A. Ross, and S. Pankanti. Biometrics: a tool for information security. *IEEE Trans. on Information Forensics and Security*, 1(2):125–143, 2006. 1

M. Y. Jeong, C. Lee, J. Kim, J. Y. Choi, K. A. Toh, and J. Kim. Changeable biometrics for appearance based face recognition. In *Proc. Conf. Biometric Consortium, Biometrics Symposium*, pages 1–5, 2006. 26

A. Juels and M. Sudan. A fuzzy vault scheme. *Designs, Codes and Cryptography*, 38(2):237–257, 2006. 3, 29, 35

A. Juels and M. Wattenberg. A fuzzy commitment scheme. *ACM Conf. on Computer and Communications Security*, pages 28–36, 1999. 3, 29, 35

T. Kanade. *Picture processing system by computer complex and recognition of human faces*. PhD thesis, Kyoto University, 1973. 1, 39

E. Kelkboom, X. Zhou, J. Breebaart, R. Veldhuis, and C. Busch. Multi-algorithm fusion with template protection. In *Proc. Int. Conf. on Biometrics: Theory, Applications, and Systems (BTAS)*, pages 1–8, 2009. 35, 36, 141

A. Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, 9:5–83, 1883. Available on-line at http://www.petitcolas.net/fabien/kerckhoffs/#english. 10, 26, 103

A. Kholmatov and B. Yanikoglu. Identity authentication using improved online signature verification method. *Pattern Recognition Letters*, 26:2400–2408, 2005. 53

Y. Kim and K. Toh. A method to enhance face biometric security. In *Proc. Int. Conf. on Biometrics: Theory, Applications, and Systems (BTAS)*, pages 1–6, 2007. 28

J. Kittler, A. Kumar, S. Sarkar, T. Boult, S. Li, D. Maltoni, and M. Vatsa, editors. *Proc. of Second International Joint Conference on Biometrics (IJCB)*, 2014. IEEE. 1

D. H. Klatt. Software for a cascade/parallel formant synthesizer. *Journal Acoustic Society of America*, 67:971–995, 1980. 21

P. Komarinski. *Automated Fingerprint Identification Systems (AFIS)*. Elsevier, 2005. 4

A. Kong, K.-H. Cheunga, D. Zhanga, M. Kamelb, and J. Youa. An analysis of BioHashing and its variants. *Pattern Recognition*, 39(7):1359–1368, 2006. 3, 29

S. Kullback and R. A. Leibler. On information and sufficiency. *The Annals of Mathematical Statistics*, 22(1): 79–86, 1951. 45

A. Kumar and A. Passi. Comparison and combination of iris matchers for reliable personal authentication. *Pattern Recognition*, 43(3):1016–1026, 2010. 55

R. L. Lagendijk, Z. Erkin., and M. Barni. Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation. *IEEE Signal Processing Magazine*, 30(1): 82–105, 2013. 24, 119

A. Levi, E. Savas, H. Yenigun, S. Balcisoy, and Y. Saygin. Biometric cryptosystem using online signatures. In *Proc. Computer and Information Sciences (ISCIS)*, volume 4263 of *LNCS*, pages 981–990, 2006. 31

G. Li, B. Yang, C. Rathgeb, and C. Busch. Towards generating protected fingerprint templates based on bloom filters. In *Proc. Int. Workshop on Biometrics and Forensics (IWBF)*, 2015. 28, 100, 106, 107, 108

A. Lin and L. Wang. Style-preserving english handwriting synthesis. *Pattern Recognition*, 40:2097–2109, 2007. 19

LivDet, 2009. http://prag.diee.unica.it/LivDet09/. 1

M. Locasto, V. Shmatikov, and U. Erlingsson, editors. *Proc. of the 37th IEEE Symposium on Security and Privacy*, 2016. 7

H. Lu, K. Martin, F. Bui, K. Plataniotis, and D. Hatzinakos. Face recognition with biometric encryption for privacy-enhancing self-exclusion. In *Proc. Int. Conf. on Digital Signal Processing (DSP)*, 2009. 30

Y. Luo, S. S. Cheung, and S. Ye. Anonymous biometric access control based on homomorphic encryption. In *Proc. Int. Conf. on Multimedia and Expo (ICME)*, pages 1046–1049, 2009. 3

D. Maio, D. Maltoni, R. Cappelli, J. Wayman, and A. Jain. FVC2002: Second Fingerprint Verification Competition. In *Proc. Int. Conf. on Pattern Recognition (ICPR)*, pages 811–814. IEEE Press, 2002a. 55

D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain. FVC2000: Fingerprint Verification Competition. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 24(3):402–412, 2002b. 41

E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri. Cancelable templates for sequence-based biometrics with application to on-line signature recognition. *IEEE Trans. on Systems Man and Cybernetics - Part A: Systems and Humans*, 40(3):525–538, 2010. 26, 27

E. Maiorana, P. Campisi, and A. Neri. User adaptive fuzzy commitment for signature template protection and renewability. *Journal of Electronic Imaging*, 17(1):011011–011011, 2008. 30

E. Maiorana, P. Campisi, and A. Neri. Feature selection and binarization for on-line signature recognition. In *Proc. Int. Conf. on Biometrics (ICB)*, pages 1219–1229, 2009. 53

E. Maiorana, G. E. Hine, and P. Campisi. Hill-climbing attacks on multi-biometrics recognition systems. *IEEE Trans. on Information Forensics and Security*, 10(5):900–915, 2015. 122, 141, 149

S. Makthal and A. Ross. Synthesis of iris images using markov random fields. In *Proc. European Signal Processing Conferende (EUSIPCO)*, 2005. 19, 83

A. Mansfield and J. Wayman. Best practices in testing and reporting performance of biometric devices. Technical report, CESG Biometrics Working Group, August 2002. (http://www.cesg.gov.uk/). 40

A. Martin, G. Doddington, T. Kamm, M. Ordowski, and M. Przybocki. The DET curve in assessment of decision task performance. In *Proc. Eurospeech*, pages 1895–1898, 1997. 41

M. Martinez-Diaz, J. Fierrez, R. P. Krish, and J. Galbally. Mobile signature verification: Feature robustness and performance comparison. *IET Biometrics*, 3:267–277, 2014. 53

L. Masek and P. Kovesi. Matlab source code for a biometric identification system based on iris patterns. Master's thesis, School of Computer Science and Software Engineering, University of Western Australia, 2003. 51, 83, 84

J. H. Mathews and K. K. Fink. *Numerical Methods Using Matlab*, chapter Numerical Optimization, pages 430–436. Prentice-Hall Inc., 2004. 64

T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. Impact of artificial gummy fingers on fingerprint systems. In *Proc. SPIE Optical Security and Counterfeit Deterrence Techniques IV*, volume 4677, pages 275–289, 2002. 2

A. Mayoue, B. Dorizzi, L. Allano, G. Chollet, J. Hennebert, D. Petrovska-Delacretaz, and F. Verdet. *Guide to biometric reference systems and performance evaluation*, chapter BioSecure multimodal evaluation campaign 2007 (BMEC 2007), pages 327–372. Springer, 2009. 1

K. Messer, J. Matas, J. Kittler, J. Luettin, and G. Maitre. XM2VTSDB: The extended M2VTS database. In *Proc. Int. Conf. on Audio and Video-Based Biometric Person Authentication (AVBPA)*, volume 964, pages 965–966, 1999. 55

N. Miura, A. Nagasaka, and T. Muyatake. Extraction of finger-vein patterns using maximum curvature points in image profiles. *IEICE Trans. on Information and Systems*, 90(8):1185–1194, 2007. 52

P. Mohanty, S. Sarkar, and R. Kasturi. From scores to face templates: A model-based approach. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 29:2065–2078, 2007. 22, 23

A. Morales, E. González, and M. A. Ferrer. On the feasibility of interoperable schemes in hand biometrics. *Sensors*, 12(2):1352–1382, 2012. 54, 71

M. Mori, A. Suzuki, A. Shio, and S. Ohtsuka. Generating new samples from handwritten numerals based on point correspondence. In *Proc. IAPR Int. Workshop on Frontiers in Handwriting Recognition (IWFHR)*, pages 281–290, 2000. 20

G. S. Morrison. Measuring the validity and reliability of forensic likelihood-ratio systems. *Science & Justice*, 51 (3):91–98, 2011. ISSN 1355-0306. 47

MTIT. Minutiae Template Interoperability Testing, FP6-2004-IST-4, 2009. http://www.mtitproject.com/index.html. 1

M. E. Munich and P. Perona. Visual identification by signature tracking. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 25(2):200–217, 2003. 20

A. Nagar. *Biometric Template Security.* PhD thesis, Michigan State University, 2012. 7

A. Nagar, K. Nandakumar, and A. Jain. Multibiometric cryptosystems based on feature-level fusion. *IEEE Trans. on Information Forensics and Security*, 7(1):255–268, 2012. ISSN 1556-6013. 33, 35, 36

R. Nagel and A. Rosenfeld. Computer detection of freehand forgeries. *IEEE Trans. on Computers*, 26(9):895–905, 1977. 39

K. Nandakumar. A fingerprint cryptosystem based on minutiae phase spectrum. In *Proc. Int. Workshop on Information Forensics and Security (WIFS)*, pages 1–6, 2010. 30

K. Nandakumar and A. K. Jain. Multibiometric template security using fuzzy vault. In *Proc. Int. Conf. on Biometrics: Theory, Applications, and Systems (BTAS)*, pages 1–6, 2008. 3, 35, 36

K. Nandakumar and A. K. Jain. Biometric template protection: Bridging the performance gap between theory and practice. *IEEE Signal Processing Magazine*, 32(5):88–100, 2015. 7, 9, 11, 33

K. Nandakumar, A. K. Jain, and S. Pankanti. Fingerprint-based fuzzy vault: Implementation and performance. *IEEE Trans. on Information Forensics and Security*, 2(4):744–757, 2007. 11, 30, 31

J. A. Nelder and R. Mead. A simplex method for function minimization. *Computer Journal*, 7:368 – 313, 1965. 22, 73

Neurotechnology. URL `http://www.neurotechnology.com/verieye.html`. 51, 83

NIST. NIST Special Publication 800-76, "Biometric Data Specification for Personal Identity Verification," Feb. 2005. 89

C. Oliveira, C. A. Kaestner, F. Bortolozzi, and R. Sabourin. Generation of signatures by deformations. In *Proc. IAPR Int. Conf. on Advances in Document Image Analysis (ICADIA)*, pages 283–298. Springer LNCS-1339, 1997. 20

M. Olsen, D. Hartung, and C. B. B. Larsen. Convolution approach for feature detection in topological skeletons obtained from vascular patterns. In *Proc. IEEE Workshop on Computational Intelligence in Biometrics and Identity Management (CIBIM)*, pages 163–167, 2011. 52

J. Ortega-Garcia, J. Fierrez, *et al.* The multi-scenario multi-environment BioSecure multimodal database (BMDB). *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 32:1097–1111, 2010. 56

M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich. SCiFI: A system for secure face identification. In *Proc. IEEE Symp. Security and Privacy*, page 239–254, 2010. 32, 33

A. Othman and A. Ross. On mixing fingerprints. *IEEE Trans. on Information Forensics and Security*, 8(1): 260–267, 2013. 20, 35, 36

P. Paillier. Public-key cryptosystems based on composite residuosity classes. In *Proc. EUROCRYPT*, pages 223–238, 1999. 32, 122, 123

B. Paltridge. Thesis and dissertation writing: An examination of published advice and actual practice. *English for Scientific Purposes*, 21:125–143, 2002. 12

V. M. Patel, N. Ratha, and R. Chellappa. Cancelable biometrics: A review. *IEEE Signal Processing Magazine*, 32(5):54–65, 2015. 9, 28, 154, 163

P. Paul and M. Gavrilova. Multimodal cancelable biometrics. In *Int. Conf. Cognitive Informatics Cognitive Computing (ICCI*CC)*, pages 43–49, 2012. 34, 36, 141

R. D. Peng. Reproducible research in computational science. *Science*, 334(6060):1226–1227, 2011. 11

J. P. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss. The FERET evaluation methodology for face-recognition algorithms. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 22(10):1090–1104, 2000a. 1, 40

P. Phillips, A. Martin, C. Wilson, and M. Przybocki. An introduction to evaluating biometric systems. *IEEE Computer*, 33(2):56–63, 2000b. 40

P. J. Phillips. Face and iris evaluations at NIST. In *CardTech/SecurTech*, May 2006. 1

P. J. Phillips, J. R. Beveridge, B. A. Draper, G. Givens, A. J. O'Toole, D. S. Bolme, J. Dunlop, Y. M. Lui, H. Sahibzada, and S. Weimer. An introduction to the good, the bad, amp; the ugly face recognition challenge problem. In *Proc. Int. Conf. on Automatic Face Gesture Recognition and Workshops (2011)*, pages 346 –353, march 2011. 1

P. J. Phillips, P. J. Flynn, J. R. Beveridge, W. T. Scruggs, A. J. O'Toole, D. Bolme, K. W. Bowyer, B. A. Draper, G. H. Givens, Y. M. Lui, H. Sahibzada, J. A. Scallan, Iii, and S. Weimer. Overview of the multiple biometrics grand challenge. In *Proc. Int. Conf. on Biometrics (ICB)*, pages 705–714, Berlin, Heidelberg, 2009a. Springer-Verlag. ISBN 978-3-642-01792-6. 1

P. J. Phillips, W. T. Scruggs, A. J. O'Toole, P. J. Flynn, K. W. Bowyer, C. L. Schott, and M. Sharpe. FRVT 2006 and ICE 2006 large-scale experimental results. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 99, 2009b. 1

J. K. Pillai, V. M. Patel, R. Chellappa, and N. Ratha. Sectored random projections for cancelable iris biometrics. In *Proc. Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1838–1841, 2010. 28

J. K. Pillai, V. M. Patel, R. Chellappa, and N. Ratha. Secure and robust iris recognition using random projections and sparse representations. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 30(9):1877–1893, 2011. 11, 27, 28

N. B. Pinto, D. G. Childers, and A. L. Lalwani. Formant speech synthesis: improving production quality. *IEEE Trans. on Acoustics, Speech and Signal Processing*, 37:1870–1887, 1989. 21

N. Poh and J. Kittler. A unified framework for biometric expert fusion incorporating quality measures. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 34(1):3–18, 2012. 33, 155, 164

N. Poh, S. Marcel, and S. Bengio. Improving face authentication using virtual samples. In *Proc. Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, 2003. 19, 20

D. V. Popel. *Synthesis and analysis in biometrics*, chapter Signature analysis, verification and synthesis inpervasive environments, pages 31–63. World Scientific, 2007. 19

M. Przybocki and A. Martin. NIST Speaker Recognition Evaluation chronicles. In J. Ortega-Garcia *et al.*, editors, *Proc. ISCA Workshop on Speaker and Language Recognition (ODYSSEY)*, pages 15–22, 2004. 1

R. Raghavendra, C. Busch, and B. Yang. Scaling-robust fingerprint verification with smartphone camera in real-life scenarions. In *Proc. Int. Conf. on Biometrics: Theory, Applications, and Systems (BTAS)*, pages 1–8, 2013. 52

R. Raghavendra, K. B. Raja, J. Surbiryala, and C. Busch. A low-cost multimodal biometric sensor to capture finger vein and fingerprint. In *Proc. IEEE Int. Joint Conf. on Biometrics (IJCB)*, pages 1–7, 2014. 52

S. Rane. Standardization of biometric template protection. *IEEE Multimedia*, 21(4):94–99, 2014. 3, 7, 10

N. Ratha, J. Connell, R. M. Bolle, and S. Chikkerur. Cancelable biometrics: A case study in fingerprints. In *Proc. Int. Conf. on Pattern Recognition (ICPR)*, volume 4, pages 370–373. IEEE, 2006. 26

N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle. Generating cancelable fingerprint templates. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 29(4):561–572, 2007. 26, 27

N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication sytems. *IBM Systems Journal*, 40:614–634, 2001. 11, 26

N. K. Ratha and V. Govindaraju, editors. *Advances in biometrics: Sensors, algorithms and systems*. Springer, 2008. 1

C. Rathgeb, F. Breitinger, and C. Busch. Alignment-free cancelable iris biometric templates based on adaptive bloom filters. In *Proc. Int. Conf. on Biometrics (ICB)*, pages 1–8, 2013a. 27, 94, 98, 100, 104, 107, 109, 117

C. Rathgeb, F. Breitinger, C. Busch, and H. Baier. On the application of bloom filters to iris biometrics. *IET Biometrics*, 2013b. (to appear). 27

C. Rathgeb and C. Busch. *New Trends and Developments in Biometrics*, chapter Multi-biometric template protection: Issues and challenges. InTech, 2012. 34

C. Rathgeb and C. Busch. Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters. *Computers & Security*, 42:1 – 12, 2014. 34, 36

C. Rathgeb, M. Gomez-Barrero, C. Busch, J. Galbally, and J. Fierrez. Towards cancelable multi-biometrics based on bloom filters: A case study on feature level fusion of face and iris. In *Proc. Int. Workshop on Biometrics and Forensics (IWBF)*, pages 1–7, 2015. 92

C. Rathgeb and A. Uhl. An iris-based interval-mapping scheme for biometric key generation. In *Proc. Int. Symp. on Image and Signal Processing and Analysis (ISPA)*, pages 511–516. IEEE, 2009. 31

C. Rathgeb and A. Uhl. Adaptive fuzzy commitment scheme based on iris-code error analysis. In *Proc. European Workshop on Visual Information Processing (EUVIP)*, pages 41–44, 2010a. 29

C. Rathgeb and A. Uhl. Attacking iris recognition: An efficient hill-climbing technique. In *Proc. Int. Conf. on Pattern Recognition (ICPR)*, 2010b. 68

C. Rathgeb and A. Uhl. Two-Factor Authentication or How to Potentially Counterfeit Experimental Results in Biometric Systems. In A. Campilho and M. Kamel, editors, *Proc. Int. Conf. on Image Analysis and Recognition (ICIAR)*, volume 6112 of *LNCS*, pages 296–305. Springer, 2010c. 29

C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 2011(3), 2011. xxv, xxv, 9, 12, 19, 24, 27, 28, 30, 34, 154, 163

C. Rathgeb and A. Uhl. Statistical attack against fuzzy commitment scheme. *IET Biometrics*, 1(2):94–104, 2012. 31

A. Ross, K. Nandakumar, and A. Jain. *Handbook of Multibiometrics*. Springer, 2006. 1, 33, 34

A. Ross and A. Othman. Visual cryptography for biometric privacy. *IEEE Trans. on Information Forensics and Security*, 6(1):70–81, 2011. 27, 28

A. Ross, J. Shah, and A. K. Jain. From template to image: reconstructing fingerprints from minutiae points. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 29:544–560, 2007. 22, 23

V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia. Direct attacks using fake images in iris verification. In *Proc. COST 2101 Workshop on Biometrics and Identity Management (BioID)*, pages 181–190. Springer LNCS-5372, 2008. 51

A.-R. Sadeghi, T. Schneider, and I. Wehrenberg. Efficient privacy-preserving face recognition. In *Information, Security and Cryptology–ICISC 2009*, pages 229–244. Springer, 2010. 32, 33

M. Savvides, B. Kumar, and P. Khosla. Cancelable biometric filters for face recognition. In *Proc. Int. Conf. on Pattern Recognition (ICPR)*, volume 3, pages 922–925, 2004. 28

W. Scheirer and T. Boult. Cracking fuzzy vaults and biometric encryption. In *Proc. Biometric Symposium*, pages 1–6, 2007. 31

B. Schneier. The uses and abuses of biometrics. *Communications of the ACM*, 48:136, 1999. 2

S. Shah and A. Ross. Generating synthetic irises by feature agglomeration. In *Proc. IEEE Int. Conf. on Image Processing (ICIP)*, pages 317–320, 2006. 19, 21, 83

K. Simoens, J. Bringer, H. Chabanne, and S. Seys. A framework for analyzing template security and privacy in biometric authentication systems. *IEEE Trans. on Information Forensics and Security*, 7(2):833–841, 2012a. 11, 12, 155, 164

K. Simoens, B. Yang, X. Zhou, F. Beato, C. Busch, E. Newton, and B. Preneel. Criteria towards metrics for benchmarking template protection algorithms. In *Proc. Int. Conf. on Biometrics (ICB)*, pages 498–505, 2012b. 9, 49

Y. Sutcu. *Template Security in Biometric Systems*. PhD thesis, New York University, 2009. 7

Y. Sutcu, Q. Li, and N. Memon. Secure biometric templates from fingerprint-face features. In *Proc. CVPR Workshop on Biometrics*, 2007. 36

Y. Sutcu, H. T. Sencar, and N. Memon. A secure biometric authentication scheme based on robust hashing. In *Proc. Workshop on Multimedia and Security*, pages 111–116. ACM, 2005. 3, 11, 31

J. Suykens, T. V. Gestel, J. D. Brabanter, B. D. Moor, and J. Vandewalle. *Least Squares Support Vector Machines*. Singapor: World Scientific, 2002. 50

TABULA RASA. Trusted biometrics under spoofing attacks, 2010. URL `http://www.tabularasa-euproject.org/`. 1

B. Tams, J. Merkle, C. Rathgeb, J. Wagner, U. Korte, and C. Busch. Improved fuzzy vault scheme for alignment-free fingerprint features. In *Proc. Int. Conf. of theBiometrics Special Interest Group (BIOSIG)*, pages 1–12, 2015. 35, 36

A. B. Teoh, A. Goh, and D. C. Ngo. Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 28(12): 1892–1901, 2006. 27, 28

A. B. Teoh and D. C. Ngo. Biophasor: Token supplemented cancellable biometrics. In *Proc. Int. Conf. on Control, Automation, Robotics and Vision (ICARCV)*, pages 1–5. IEEE, 2006. 29

A. B. J. Teoh and J. Kim. Secure biometric template protection in fuzzy commitment scheme. *IEICE Electronics Express*, 4(23):724–730, 2007. 30

A. B. J. Teoh, Y. W. Kuan, and S. Lee. Cancellable biometrics and annotations on biohash. *Pattern Recogn.*, 41 (6):2034–2044, 2008. ISSN 0031-3203. 29

A. B. J. Teoh, D. C. L. Ngo, and A. Goh. Personalised cryptographic key generation based on FaceHashing. *Computers And Security*, (23):606–614, 2004. 3, 28, 30, 31

The Hong Kong University of Science and Technology, Department of Computer Science. Ust hand image database. (Provided by Dr. Helen Shen). 54, 71

S. Theodoridis and K. Koutroumbas. *Pattern Recognition*. Academic Press, 2008. 14, 40, 92, 120

M. Tistarelli, S. Z. Li, and R. Chellappa, editors. *Handbook of Remote Biometrics for Surveillance and Security*. Springer, 2009. 1, 6

M. Tistarelli and D. Maltoni, editors. *Proc. of Second IEEE Workshop on Automatic Identification Advanced Technologies (AutoID)*, 2007. IEEE Press. 1

B. Ton and R. Veldhuis. A high quality finger vascular pattern dataset collected using a custom designed capturing device. In *Proc. Int. Conf. on Biometrics (ICB)*, pages 1–5, 2013. 55

J. Troncoso-Pastoriza and F. Perez-Gonzalez. Secure signal processing in the cloud: enabling technologies for privacy-preserving multimedia cloud processing. *IEEE Signal Processing Magazine*, 30(2):29–41, 2013. 32

J. R. Troncoso-Pastoriza, D. Gonzalez-Jimenez, and F. Perez-Gonzalez. Fully private noninteractive face verification. *IEEE Trans. on Information Forensics and Security*, 2013. 33

TURBINE. Trusted revocable biometrics identities, 2007. 7

P. Tuyls, B. Skoric, and T. Kevenaar, editors. *Security with Noisy Data. On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*. Springer, 2007. 24

A. Uhl and P. Wild. Weighted adaptive hough and ellipsopolar transforms for real-time iris segmentation. In *Proc. Int. Conf. on Biometrics (ICB)*, pages 1–8, 2012. 51

US CITeR. CITeR: Center for identification technology research, 2011. 1

J. van Beek. ePassports reloaded. In *Black Hat USA Briefings*, 2008. 89

P. Vandewalle, J. Kovačević, and M. Vetterli. Reproducible research in signal processing. *IEEE Signal Processing Magazine*, 26(3):37–47, 2009. 11

S. Venugopalan and M. Savvides. How to generate spoofed irises from an iris code template. *IEEE Trans. on Information Forensics and Security*, 6(2):385–395, June 2011. 2, 20, 21, 22, 23, 65, 66, 68

E. Verbitskiy, P. Tuyls, C. Obi, and B. Schoenmakers. Key extraction from general nondiscrete signals. *IEEE Trans. on Information Forensics and Security*, 5(2):269–279, 2010. 35

C. Vielhauer, R. Steinmetz, and A. Mayerhoefer. Biometric hash based on statistical features of online signatures. In *Proc. Int. Conf. on Pattern Recognition (ICPR)*, volume 1, pages 123–126, 2002. 30, 31

B. Vijaya-Kumar, S. Prabhakar, and A. Ross, editors. *Proc. of Fifth Conference on Biometric Technology for Human Identification (BTHI V)*, 2008. SPIE. 1

H. Wang and L. Zhang. Linear generalization probe samples for face recognition. *Pattern Recognition Letters*, 25:829–840, 2004. 20

J. Wang, C. Wu, Y.-Q. Xu, H.-Y. Shum, and L. Ji. Learning-based cursive handwriting synthesis. In *Proc. IAPR Int. Workshop on Frontiers of Handwriting Recognition (IWFHR)*, pages 157–162, 2002. 20

Z. Wei, T. Tan, and Z. Sun. Synthesis of large realistic iris databases using patch-based sampling. In *Proc. Int. Conf. on Pattern Recognition (ICPR)*, pages 1–4, 2008. 19

H. R. Wilson, G. Loffler, and F. Wilkinson. Synthetic faces, face cubes, and the geometry of face space. *Vision Research*, 42(34):2909–2923, 2002. 20

X. Wu, N. Qi, K. Wang, and D. Zhang. A novel cryptosystem based on iris key generation. In *Proc. Int. Conf. on Natural Computation (ICNC)*, volume 4, pages 53–56, 2008a. 30, 31

X. Wu, K. Wang, and D. Zhang. A cryptosystem based on palmprint feature. In *Proc. Int. Conf. on Pattern Recognition (ICPR)*, pages 1–4, 2008b. 30, 31

H. Xu, R. Veldhuis, A. Bazen, T. A. M. Kevenaar, T. Akkermans, and B. Gokberk. Fingerprint verification using spectral minutiae representations. *IEEE Trans. on Information Forensics and Security*, 4(3):397–409, 2009a. 52

H. Xu, R. Veldhuis, T. A. M. Kevenaar, and T. A. H. M. Akkermans. A fast minutiae-based fingerprint recognition system. *IEEE Systems Journal*, 3(4):418–427, 2009b. 52

B. Yang and C. Busch. Parametrized geometric alignment for minutiae-based fingerprint template protection. In *Proc. Int. Conf. on Biometrics: Theory, Applications, and Systems (BTAS)*, pages 1–6, 2009. 52

B. Yang, C. Busch, D. Gafurov, and P. Bours. Renewable minutiae templates with tunable size and security. In *Proc. Int. Conf. on Pattern Recognition (ICPR)*, pages 878–881, 2010. 52

A. C.-C. Yao. How to generate and exchange secrets. In *Proc. Annual Symposium on Foundations of Computer Science (SFCS)*, pages 162–167, 1986. 32

S. Ye, Y. L. ad J. Zhao, and S. S. Cheung. Anonymous biometric access control. *EURASIP Journal on Information Security*, 2009:1–17, 2009. 32

S.-J. Yen, Y.-C. Wu, J.-C. Yang, Y.-S. Lee, C.-J. Lee, and J.-J. Liu. A support vector machine-based context-ranking model for question answering. *Information Sciences*, 224:77–87, 2013. 50

D. Y. Yeung, H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto, and G. Rigoll. SVC2004: First International Signature Verification Competition. In D. Zhang and A. K. Jain, editors, *Proc. IAPR Int. Conf. on Biometric Authentication (ICBA)*, pages 16–22. Springer LNCS-3072, 2004. 1

Y. Yin, L. Liu, and X. Sun. SDUMLA-HMT: a multimodal biometric database. *Biometric Recognition*, pages 260–268, 2011. 56

E. Yörük, E. Konkoglu, B. Sankur, and J. Darbon. Shape-based hand recognition. *IEEE Trans. on Image Processing*, 15:1803–1815, 2006. 50, 73

Z. Zeng and P. Watters. A novel face hashing method with feature fusion for biometric cryptosystems. In *Proc. Eurorpean Conf. on Universal Multiservice Networks, ECUMN*, pages 439–444. IEEE, 2007. 30

W. Zhang, S. Shan, *et al.* Local gabor binary pattern histogram sequence (LGBPHS): a novel non-statistical model for face representation and recognition. In *Proc. Int. Conf. on Computer Vision, ICCV*, volume 1, pages 786–791, 2005. 52

X. Zhou. *Privacy and Security Assessment of Biometric Template Protection.* PhD thesis, Technische Universität, Darmstadt, 2012. 7

H. Zhu, X. Meng, and G. Kollios. Privacy preserving similarity evaluation of time series data. In *Proc. Int. Conf. on Extending Database Technology (EDBT)*, pages 499–510, 2014. 128

K. Zuiderveld. Contrast limited adaptive histogram equalization. *Graphic Gems IV*, pages 474–485, 1994. 52

J. Zuo, N. A. Schmid, and X. Chen. On generation and analysis of synthetic iris images. *IEEE Trans. on Information Forensics and Security*, 2:77–90, 2007. 19, 21